



PROGRAM MATERIALS

Program #29119

June 19, 2019

Cutting Edge Topics in Cyberinsurance Coverage

**Copyright ©2019 by Jordan Rand, Esq. - Klehr Harrison
Harvey Branzburg LLP and Austin Morris Jr. - Morris Risk
Management LLC. All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969



**KLEHR HARRISON
HARVEY BRANZBURG_{LLP}**

Business Law at Business Speed[®]



DATA BREACH
— NINJA.com —

Jordan Rand

215-569-3024

jrand@klehr.com

www.databreachninja.com

MORRIS

R I S K M A N A G E M E N T

Austin Morris, Jr.
215-947-9200
austin.morris@morrisrisk.com
www.morrisrisk.com



KLEHR HARRISON
HARVEY BRANZBURG^{LLP}

The Cyber Security Market

2004 - \$3B

2015 - \$75B

2018 - \$114B

2019 - \$124B

2025 ~ \$300B - \$1T



Drivers

Actual and Perceived Heightened Security Risks
Regulatory Compliance
Customer/Client Expectations



Bad News...IT Won't Work

(at least, not always)

University of Maryland A. James Clark School of Engineering Study (2007)

- **Computers studied attached 2,244 times/day (every 39 seconds)**
- **Brute force attacks – software that attacks large numbers of computers by guessing the most common usernames and passwords (“dictionary scripts”)**
 - **Top usernames: (1) Root; (2) admin; (3) test; (4) guest; and (5) info**
 - **Forty-three percent of password guessing attempts simply re-enter the username**
 - **Interesting side note: UMD suffered a breach in 2014 that compromised 300,000 records of faculty, staff and students**
- **More recently...**
 - **Thirty-One percent of organizations have experienced cyber attacks**
 - **Ransomware attacks are growing more than 350% annually, with successful attacks occurring every 14 seconds at a likely total cost in 2019 of \$11.5 billion**
 - **1 in 13 web requests lead to malware**

Source: “60 Must-Know Cybersecurity Statistics for 2019,” Rob Sobers (Varonis April 17, 2019)



Cost of a data breach

NetDilligence 2018 Cyber Claims Study

1,201 claims from 2013 – 2017

Average - \$603,900

Median - \$61,200

IBM/Ponemon 2018 Cost of Data Breach Study

Average \$3.86M

Verizon 2015 Data Breach Investigations Report

We really can't say...



RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	\$1,170	\$18,120	\$25,450	\$35,730	\$555,660
1,000	\$3,110	\$52,260	\$67,480	\$87,140	\$1,461,730
10,000	\$8,280	\$143,360	\$178,960	\$223,400	\$3,866,400
100,000	\$21,900	\$366,500	\$474,600	\$614,600	\$10,283,200
1,000,000	\$57,600	\$892,400	\$1,258,670	\$1,775,350	\$27,500,090
10,000,000	\$150,700	\$2,125,900	\$3,338,020	\$5,241,300	\$73,943,950
100,000,000	\$392,000	\$5,016,200	\$8,852,540	\$15,622,700	\$199,895,100



So what are you going to do about it?

Besides an intimidating eyebrow raise

- ✓ **IT Investment**
- ✓ **Employee Training**
- ✓ **Reduce Response Time**

and

- ✓ **Transfer Risk**



Don't We Already Have It?

Maybe not in your commercial general liability policy.

- *Zurich Am. Ins. Co. v. Sony Corp.*, No. 651982/2011 (N.Y. Supreme Court Feb. 21, 2014) (granting summary judgment for insurer and holding CGL policy did not cover claims arising out of 2011 hacking of PlayStation on-line services that compromised millions of users' personal information)
- CG 21 06 05 14 (Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – With Bodily Injury Exception) (excluding coverage “for injury or damage arising out of any access to or disclosure of any person’s or organization’s confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.”)
- *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*, 337 F.Supp.3d 1176 (M.D. Fla. 2018) (holding CGL policy did not provide defense under personal injury coverage because unauthorized disclosure of credit card information was caused by third party intrusion rather than by insured’s actions, thereby failing to establish a “publication” by the insured in violation of third parties’ rights of privacy)



What About Commercial Crime Coverage?

Eh...

- ***Schmidt v. Travelers*, 101 F.Supp.3d 768 (S.D. Ohio 2015)** (granting summary judgment for insurer because commercial crime policy's "voluntary parting" exclusion barred coverage for wire fraud effectuated through email impersonation of a lawyer's client)
- ***Apache Corp. v. Great American Insurance Co.*, 662 Fed.Appx. 252 (5th Cir. 2016)** (affirming summary judgment for insurer based on interpretation of computer fraud provision as not covering \$7 million in wire transfers induced by fraudulent emails deemed "incidental" to general fraud rather than direct cause of the loss)
- ***Interactive Communications International, Inc. v. Great American Insurance Co.*, 731 Fed.Appx. 929 (11th Cir. 2018)** (granting summary judgment for insurer because although fraudsters manipulated insured's computer operated interactive voice response system to cause fraudulent wires, the loss was not "directly" caused by the use of computers, as that was the first in a multi-step process that concluded with the fraudulent wires)
- ***But see American Tooling Center, Inc. v. Travelers*, 895 F.3d 455 (6th Cir. 2018)** (reversing trial court and granting summary judgment for insured based on interpretation of computer fraud coverage deemed to include claims based on use of fraudulent emails to induce insured to wire nearly \$900,000 to criminal impersonating one of its vendors); ***Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F.Supp.3d 471 (S.D.N.Y. 2017)** (granting summary judgment for insured because crime policy covered nearly \$5 million wire induced by email fraud)



D&O, E&O???

- **Explicit Cyber exclusions**: Increasingly excluding “privacy incidents”
- **Other insurance**: Provisions that bar coverage where other insurance is applicable or that require “adequate” other insurance
 - ***St. Paul Fire & Marine Insurance*** – Carrier argued unsuccessfully that the ready and known availability of cyber insurance for data breach losses is itself an indication that CGL policies are not intended to cover those losses and the insured *actually purchased* cyber insurance since 2015-16.
 - Relying on cases holding that courts should construe insurance policies so as *not* to find duplicative coverage, St. Paul argued that the CGL policies must be interpreted so as not to provide coverage for data breach losses because the insured’s Beazley policy did provide that coverage.



The Market

- **2019 - \$3-4 Billion...By 2024: \$17 Billion**
- **Premiums – Cost Per Million of Coverage**
 - Drivers: Industry, Annual Revenue, Nature of Data
- **Limits - \$1M - \$20M/carrier, with towers into the \$100 Millions**
 - Drivers: Industry, Annual Revenue, Nature of Data
- **“How much does Cyber/Data Breach Insurance Cost?,”
Christine Marciano (Cyber Data Risk Managers April 2018)**
 - Highest Revenue: A pharmaceutical benefits management company with annual revenues of \$4B bought a policy with a \$5M limit for a premium of \$84,000.
 - Highest Limits: A data storage center with annual revenues of \$15M bought a policy with a \$20M limit for a premium of \$120,000.
 - The \$1M Phenomenon: 18 of 34 clients bought \$1M policies. Even more interesting, those clients’ annual revenues ranged from \$100,000 to \$100M.



The Coverage

- Forensic Investigation
- Data Recovery
- Information Assets
- BEC Losses
- Breach Notification
- Credit Monitoring
- Network Business Interruption
- Network Extortion
- Public Relations/Crisis Management
- Defense and Liability
- Regulatory Investigations and Penalties

196

ERIC ALLEN

CB PHILADELPHIA EAGLES

HT: 5'10" WT: 180 COLLEGE: ARIZONA STATE
BORN: 11-22-65, SAN DIEGO, CA

FOOTBALL NEWS **SKILLS RATING SYSTEM**

SPEED	COVERAGE	VS. RUN	HANDS
9.6	9.3	8.4	9.5

KEY STAT: Had two interceptions in last season's playoff victory over New Orleans...The speedy Allen has been labeled by Philadelphia coach Rich Kotite as the best cornerback he's ever been around...Opposing quarterbacks are afraid to throw in his direction...Has appeared in Pro Bowl in three of the last four seasons.

COMPLETE NFL RECORD

	DEFENSIVE RECORD						
	SACKS	TCKLS	SOLO	INT	YDS	FF	FR
1992	0.0	72	42	4	49	1	2
CAREER	0.0	287	220	25	220	1	4

1988 TOPPS ROOKIE CARD

Topps Stadium Club Team NFL

B ©1993 THE TOPPS COMPANY, INC.



Forensic Investigation and Data Recovery



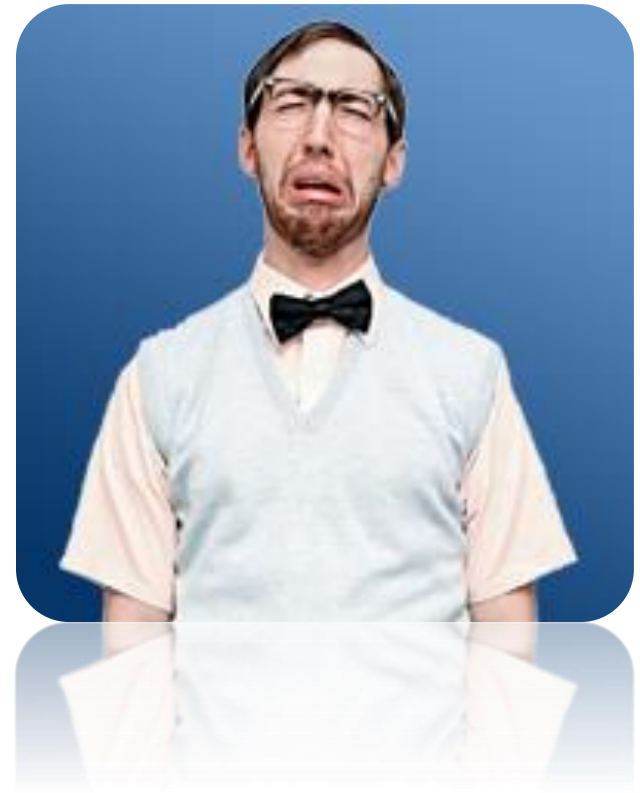
“reasonable and necessary expenses the Insured Entity incurs to conduct an investigation of its Computer System by a Third Party to determine the source of cause of the Data Privacy Wrongful Act or Network Security Wrongful Act.”



And If The Nerds Can't Fix It

Information Asset Coverage

- **“actual information asset loss...resulting directly from injury to information assets” that results from “a failure of security of your computer system”**
- **Information Asset Loss = “software or electronic data, including without limitation, customer lists and information, financial, credit card or competitive information, and confidential or private information” “that are altered, corrupted, destroyed, disrupted, deleted or damaged.”**



BEC Losses

- **FBI Definition:** “sophisticated scam targeting both businesses and individuals performing wire transfer payments...[that] is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer engineering techniques to conduct unauthorized transfers of funds.”
- **Common examples:** Emails that appear to come from a CEO or CFO directing an employee to pay a fake vendor and scammers posing as title insurance representatives sending last-minute changes in wiring instructions to real estate purchasers.
- **Between 2013 and 2018, BECs accounted for over \$12.5 billion in *reported* losses globally, but data is limited to self-reported information received through its Internet Complaint Center, or IC3.**
- **Of these losses, there have been 41,058 incidents in the United States accounting for nearly \$3 billion in losses. This figure represents more than half of fraud-related losses reported to the FBI during this five-year period.**

**Source: Federal Bureau of Investigation Public Service Announcement
(July 12, 2018)**



Can't We Just Keep This Between Us?

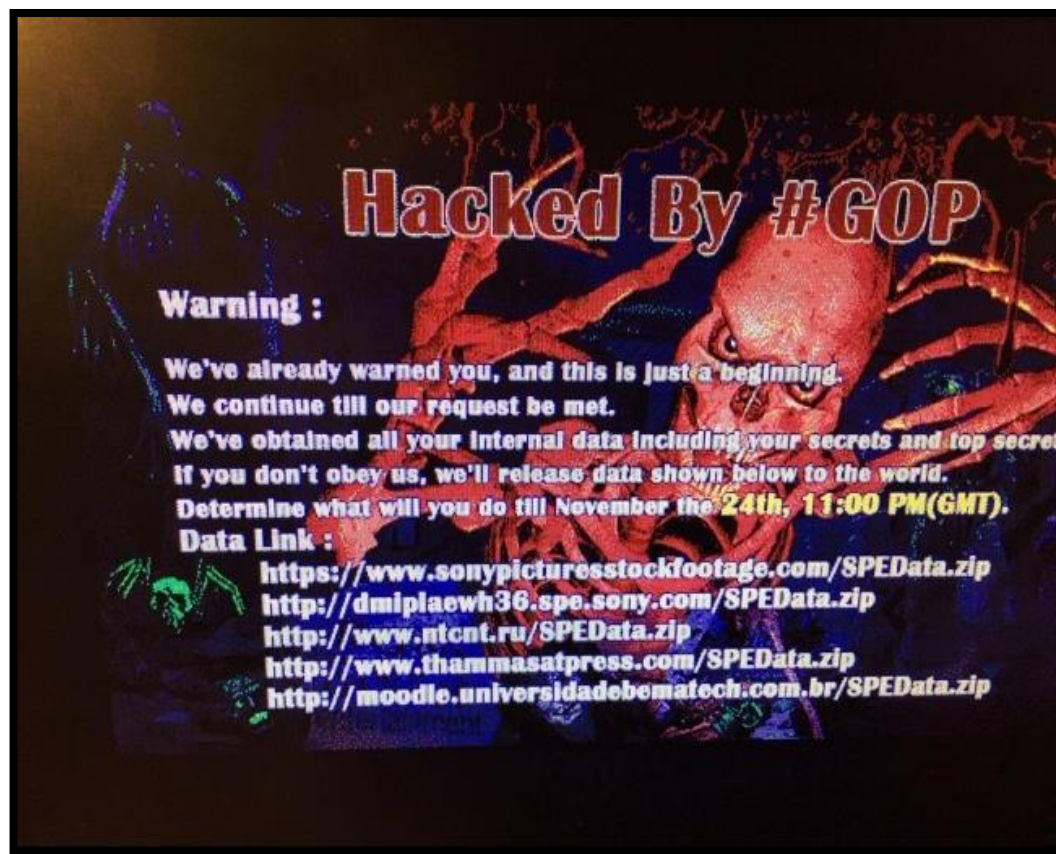
No. Data Breach Notification.

- Now in every state
 - See https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf
- Gramm-Leach-Bliley for Financial Institutions
- Health Insurance Portability and Accountability Act of 1997 for Healthcare Entities
- EU General Data Processing Regulation (May 2017)



Business Network Interruption

“business interruption loss...which the insured sustains during the period of recovery...resulting directly from a material interruption (the actual measurable interruption or suspension of the insured’s computer system) which is directly caused by a failure of security.”



Cyberextortion/Ransomware

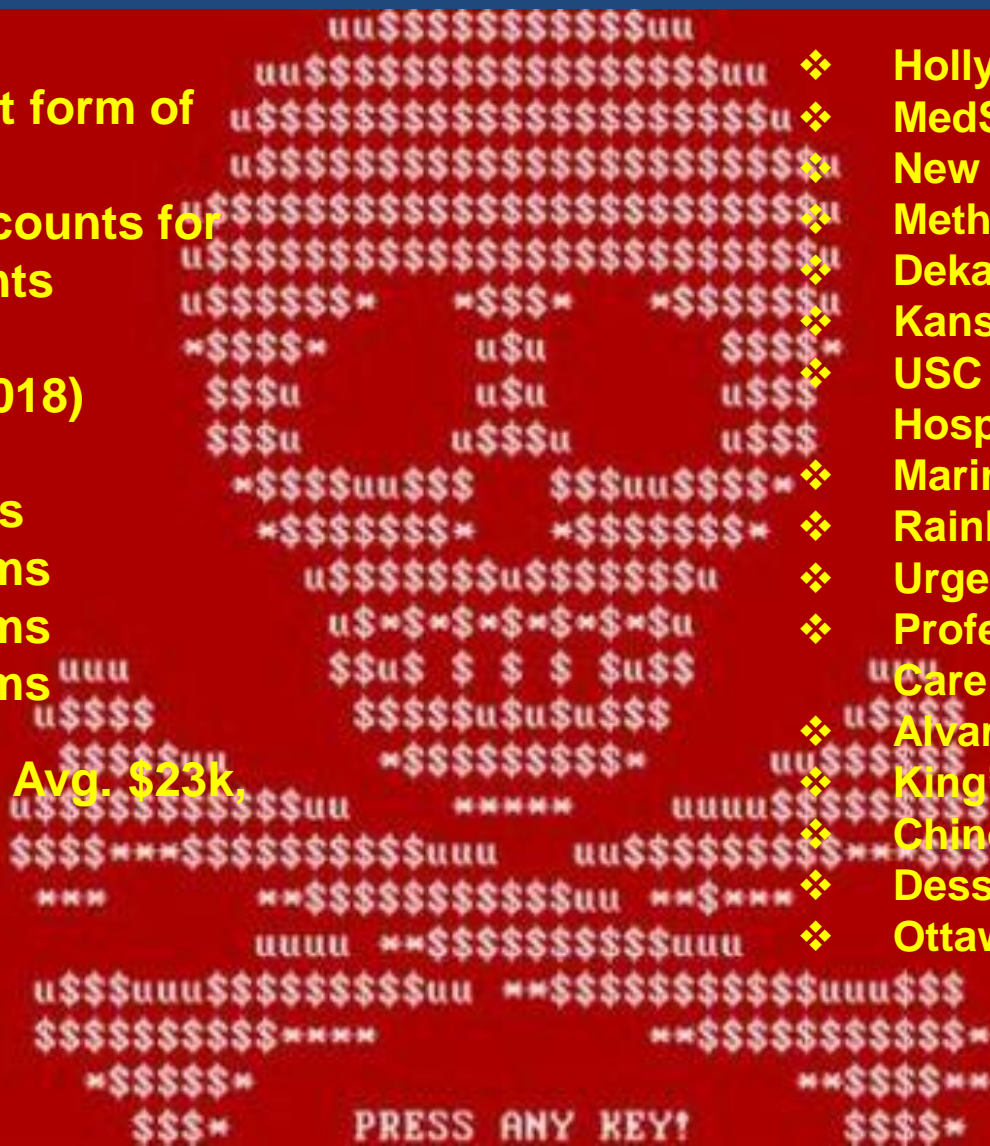
Verizon (2018)

- most prevalent form of malware
- Healthcare accounts for 85% of incidents

NetDilligence (2018)

- 2013 – 1 claim
- 2014 – 7 claims
- 2015 – 19 claims
- 2016 – 68 claims
- 2017 – 91 claims
- Ransom Cost: Avg. \$23k, Median \$13k

❖ Hollywood Presbyterian
❖ MedStar Hospitals
❖ New Jersey Spine Center
❖ Methodist Hospital
❖ Dekalb Health
❖ Kansas Heart Hospital
❖ USC Keck and Norris Hospitals
❖ Marin Healthcare District
❖ Rainbow Children's Clinic
❖ Urgent Care Clinic of Oxford
❖ Professional Dermatology Care
❖ Alvarado Medical Center
❖ King's Daughter's Health
❖ Chino Valley Medical Center
❖ Dessert Valley Hospital
❖ Ottawa Hospital



Crisis Management/Public Relations

Yahoo! (2016)

Equifax (2017)

Facebook (2018)



Defense and Liability

Target - \$10M

Anthem - \$115M

Yahoo! - \$50M...No!

Equifax Securities/Shareholder Litigation



Regulatory Investigation/Penalties

- **Federal Trade Commission**
- **Department of Health and Human Services – Office of Civil Rights**
- **State Attorneys General**
- **Payment Card Industry**
- **EU Data Privacy Authorities**
- **Uber – 57M user and 600,000 driver accounts breached - \$148M in fines for violation of breach notice laws**
- **Yahoo! – SEC fined \$85M, again non-disclosure**
- **Anthem – \$16M – Department Health and Human Services – Office of Civil Rights**
- **PCI fines – PF Chang's - \$2M**



The Hostile Acts/Terrorism Exclusion

Mondelez (NotPetya 2017)

- **Zurich coverage: “physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the introduction of malicious code”**
- **Exclusion: “a hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any: (i) government or sovereign power (de jour or de facto); (ii) military, naval, or air force; or (iii) agent or authority of any party specified in I or II above”**

Sony (The Interview 2014)

- **AIG coverage: for “a failure or violation of the security of a Computer System that: (A) results in, facilitates or fails to mitigate any: (i) unauthorized access or use; (ii) denial of service attack; or (iii) receipt, transmission or behavior of a malicious code; or (B) results from the theft of a password or access code from an Entity Insured’s premises, the Computer System, or an officer, director or employee of an Entity Insured by non-electronic means. “Security Failure” shall not include any of the foregoing that results, directly or indirectly, from any: (1) natural or man-made earth movement, flood, earthquake, seaquake, shock, explosion, tremor, seismic event, lightning, fire, smoke, wind, water, landslide, submarine landslide, avalanche, subsidence, sinkhole collapse, mud flow, rock fall, volcanic activity, including eruption and lava flow, tidal wave, hail, or act of God; or (2) satellite or other infrastructure failure”**
- **Exclusion: “arising out of...war, invasion, military action...political disturbance, civil commotion, riot, martial law, civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power...”.**



Contractual Liability Exclusion

***P.F. Chang's v. Federal Insurance Co.,
2016 WL 3055111 (D. Ariz. May 31, 2016)***

- **2014 hack exposes credit card numbers of 60,000 customers**
- **P.F. Chang's has Chubb cyber-specific policy that covers forensic investigation, litigation defense and other costs up to \$1.7M, but not \$2M in PCI fines for which it had to indemnify its credit card processor**
- **Exclusion: Insurer “shall not be liable for any Loss on account of any Claim...based upon, arising from or in consequence of any...liability assumed by any Insured under any contract or agreement.”**
- **Court found that P.F. Chang's obligation to pay the PCI fines arose from its contractor with its processor – no coverage**



Contractual Liability Exclusion

Caveat: Not a cyberinsurance policy

Spec's Family Partners Ltd.,
2018 WL 3120794 (5th Cir. June 25, 2018)

- **2012-14 hack exposes credit card numbers of customers...**
- **Millions in PCI fines...**
- **Contractual liability exclusion...**
- **But... “Simply put, the district court’s assertion that ‘Spec’s fail[ed] to allege any facts that show it would be liable or have any form of privity or obligation to pay damages to First Data for any other reason tha[n] those that arise out of contractual liability’ rewrites the allegations, ignoring statements in the demand letters that do not depend upon the Merchant Agreement, such as Spec’s *negligence* in not complying with the Payment Card Industry Data Security requirements and demands for a type of non-monetary relief not contemplated by the Merchant Agreement.”**



Contractual Liability Exclusion

Dittman v. University of Pittsburgh Medical Ctr.,
2018 WL 6072199 (Pa. Nov. 21, 2018)

- Class action by over 60,000 UPMC employees whose personal information was compromised in a data breach
- Employees alleged UPMC failed to utilize reasonable measures to protect their personal data
- Trial court holds no independent common duty to guard duty...Superior Court affirms
- Supreme Court reverses: “Employees have asserted that UPMC breached its common law duty to act with reasonable care in collecting and storing their personal and financial information on its computer systems. *As this legal duty exists independently from any contractual obligations between the parties*, the economic loss doctrine does not bar Employees’ claim.”
- What was the Fifth Circuit just saying about potential other types of liability arising out of data breaches?



Contractual Liability Exclusion

So what...

- Most cyberinsurance policies contain language like this: “This insurance does not apply to...Loss on account of any Claim made against any Insured...based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. *However, this exclusion does not apply to your liability that would have attached in the absence of such contract of agreement.*”
- After *Dittman* and *Spec’s*, is it easier to argue that data breach related liability “would have attached in the absence of such contract”?



The Cyber Endorsement

Camp's Grocery, Inc. v. State Farm,
2016 WL 6217161 (N.D. Ala. Oct. 25, 2016)

- **Hackers compromise customer credit card information**
- **Credit unions sue Camp's for damages related to card reissuance, fraud reimbursement and fraud prevention expenses**
- **But Camp's purchased a "Computer Programs and Electronic Data Extension of Coverage" in conjunction with its traditional insurance portfolio**
- **Court held that the endorsement covered only Camp's first party losses related to the breach, and not third party defense or liabilities**
- **More commonly, the opposite is true**



Are you done yet?
Yes.

Thanks for listening and...

The cases, sample insurance policies, data breach studies and articles referenced are available at

<https://www.databreachninja.com/resources/>

for your convenience, many are also available in the following pages.

Now finish your lunch and get back to work...



Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



APRIL 18, 2016

"Travelers v. Portal Healthcare Solutions – NBD"

By **Jordan M. Rand**

FYI, NBD is "internet slang" for "no big deal." "Internet slang" is what my little brother uses in text messages.

Anyway.

Last week, the **Fourth Circuit affirmed an Eastern District of Virginia** ruling that Travelers had a duty to defend Portal Healthcare Solutions with respect to a class action data breach lawsuit filed after patients found their medical records online, sans permission. The opinion analyzed a commercial general liability policy (CGL), specifically the "publication" issue that was also at the forefront in the 2015 Sony Playstation coverage dispute. In Sony, a New York City trial court held that CGL carriers had no duty to defend a data breach class action, a ruling many saw as a sign that the days of finding data breach coverage in CGL policies was coming to an end. There have therefore been a number of commentators suggesting that Travelers is a pendulum swing in the other direction, a sign that the viability of data breach coverage under CGL policies remains.

My opinion? Nope.

The policies in *Travelers* were issued in January 2012 and January 2013. On May 1, 2014, CGL policies began incorporating ISO standard exclusion CG 21 06 05 14, which excludes, under CGL coverages A and B ("B" was involved in *Sony* and *Travelers*), coverage for "injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."

The **commentary** on this exclusion's effect:

"Translation: No coverage for you if someone sues you for a data breach... This prevents an insurer from having to cover a loss that might fit within the policy's definition of personal and advertising injury [Coverage B]. ISO's explanatory memorandum described the impact of the endorsement this way:

"With respect to bodily injury and property damage arising out of access or disclosure of confidential or personal information, these changes are a reinforcement of coverage intent. As discussed above, damages related to data breaches, and certain data-related liability, are not intended to be covered under the abovementioned coverage part. These types of

damages may be more appropriately covered under certain stand-alone policies including, for instance, an information security protection policy or a cyber liability policy.

To the extent that any access or disclosure of confidential or personal information results in an oral or written publication that violates a person's right of privacy, this revision may be considered a reduction in personal and advertising injury coverage."

Travelers is not a trend reversal. It is among the few lawsuits lingering in the court system involving outdated CGL policy language. Your CGL policy is almost assuredly a claims-made policy, meaning that a data breach lawsuit today would only *potentially* be covered under your most recent policy (not the one in effect when the breach actually occurred). Because your policy likely contains CG 21 06 05 14 and/or similar language, *Travelers* isn't going to be much help. In short, *Travelers* is not the beginning of a new trend. It is far more likely the end of an old one.

Posted in: **Legal Developments and Policy Terms**

Comments are closed.

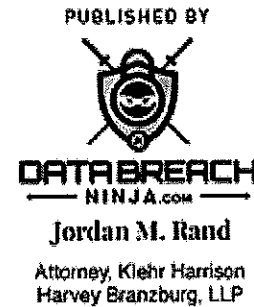
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



JUNE 10, 2016

"P.F. Chang's On the Hook for Contractual Liabilities"

By **Jordan M. Rand**

On May 31, 2016, the U.S. District Court for the District of Arizona held that P.F. Chang's obligation to pay its credit card processor nearly \$2M following a 2014 data breach was contractual, and therefore not covered under its cyberinsurance policy. Ouch. Let's back up.

In 2014, hackers posted the credit card numbers of 60,000 P.F. Chang's customers on the internet. P.F. Chang's had a Chubb cyberinsurance policy in place, for which it paid a \$134,052.00 annual premium. Chubb paid P.F. Chang's \$1.7M in policy benefits to cover forensic investigation, litigation defense and other costs, *but that was less than half of the cost of this breach.*

Really? Yes, really.

Like most businesses, P.F. Chang's contracts with a third-party credit card processor, Bank of America Merchant Services ("BAMS") to process credit card payments. BAMS, in turn, contracts with credit card associations – here, MasterCard – to be able to process those transactions. MasterCard's contract with BAMS makes BAMS liable for fees and penalties following a data breach. BAMS, in turn, has contractual indemnification for those costs from P.F. Chang's. It's the circle of credit card processing life. Follow?

After the breach, MasterCard fined BAMS nearly \$2M for the costs associated with addressing fraudulent charges and notifying affected individuals. BAMS turned to P.F. Chang's for indemnification, and P.F. Chang's turned to Chubb for coverage. No dice.

The Chubb policy, like many cyberinsurance policies, excludes coverage for contractually assumed liability. This is standard in Commercial General Liability ("CGL") policies, and since those forms are being used as the starting point for many cyber policies, that concept has bled into cyberinsurance policies. P.F. Chang's argued that the exclusion didn't apply because it would have been responsible for BAMS' claims even absent a contract, but the Court disagreed. In rejecting P.F. Chang's position, the Court "turned to cases analyzing commercial general liability policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same."

CGL and cyberinsurance policy principles are not the same. The liabilities covered under a CGL policy (e.g., slip-and-fall, property damage) are generally not the types of liabilities that would ever be contractual. Therefore, if a CGL insured assumed an unusual liability by contract, it would make sense to exclude that liability from coverage because the carrier would not have contemplated that exposure when underwriting

the policy. Data breaches are a different animal. 'Fundamentally.' While the data breach liability landscape is in constant flux, contractual liability is a major source of data breach related liability. This is particularly true as companies increasingly attempt to shift this risk to co-contracting parties.

Like several other standard CGL provisions (e.g., the **acts of war/terror exclusion**), contractual liability exclusions may eliminate coverage that most insureds would otherwise expect from a cyberinsurance policy. Negotiate for the removal or revision of this kind of language. Most carriers are willing to revise policy terms, and language varies greatly from carrier to carrier. Don't just compare premiums. Keep an eye out for CGL spill-over that doesn't belong, and use language variation as a major factor when policy shopping.

And order the Mongolian beef. It is delicious.

Posted in: **Legal Developments and Policy Terms**

Comments are closed.

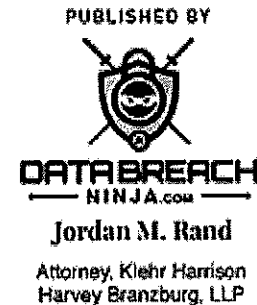
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



NOVEMBER 1, 2016

"The Danger of the Cyber Endorsement"

By **Jordan M. Rand**

For relatively little expense, insureds can often add cyber endorsements to traditional CGL, professional liability or other insurance policies. On October 25, 2016, the Northern District of Alabama issued a decision in *Camp's Grocery, Inc. v. State Farm*, one of the few decisions interpreting cyber coverage to date, that demonstrates why insureds should be wary of opting for cyber endorsements instead of stand-alone policies. Docket No. 4:16-cv-0204, 2016 WL 6217161.

Camp's had a series of no good, very bad days. First, hackers accessed its network and compromised customers' credit card, debit card and check card information. Yipes. Then, three credit unions sued Camp's to recover card reissuance, fraud reimbursement and fraud prevention expenses. Double yipes. Finally, Camp's tendered the claim to State Farm, which informed Camp's that the Computer Programs and Electronic Data Extension of Coverage and related endorsements to its property and casualty policy only covered Camp's first party data breach losses. The endorsements did not cover, in State Farm's view, third party liability claims like the credit unions'.

The court agreed. It held that State Farm and no duty to defend or indemnify Camp's with respect to the credit union lawsuit. It explained that "[i]nsurance contracts generally are assigned to one of two classes: either 'first party coverage' or 'third party coverage'...'First party coverage' pertains to loss or damage sustained by an insured to its property...In contrast, if the insurer's duty to defend and pay runs to a third party claimant who is paid according to a judgment or settlement against the insured, then the insurance is classified as 'third party insurance.' Thus, wholly different interests are protected by 'first-party coverage' and 'third-party coverage'." In holding that Camp's endorsements offered only first party coverage, the court essentially held that Camp's had no coverage since it was only attempting to deal with the credit unions' third party claims.

First party coverage *is* important in cyber-land. It can cover forensic investigations to determine the source of a breach and stop it, repair of damaged or lost electronic data, breach notice reporting costs and other significant expenses. But third party coverage is also critical. It covers lawsuits like the credit unions' against Camp's, and even regulatory investigations and fines (the latter is admittedly kind of a blend of first and third party coverage, but it's also not likely to be in inexpensive endorsements to traditional insurance policies). The importance of both sets of coverage is why many cyberinsurance policies are a hybrid of both first and third party insurance.

Without stating a position on the Camp's result, I can say that I've seen many endorsements, particularly to professional liability policies, that provide only third party coverage. In Camp's, the court deemed the endorsement to provide only first party coverage. If you're trying to save a few bucks by adding cyber coverage to other insurance, do so with caution. Both first and third party coverage is critical, and, like so many things, you very well may get only what you pay for...

Posted in: **Legal Developments**

Comments are closed.

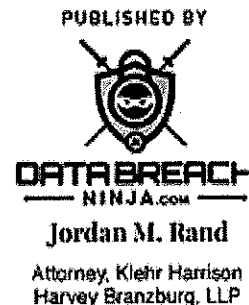
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



JUNE 27, 2018

To Be ExSPECted? Or not to be?

By Jordan M. Rand

Like a brown-paper-bag-wrapped birthday present, the Fifth Circuit's June 25th decision in **Spec's v. Hanover** arrived in my in-box with a resounding 'meh.' You see, I get daily emails from Westlaw attaching opinions that may or may not implicate cyberinsurance coverage law. I use the broadest search terms imaginable to make sure I don't miss anything by being under-inclusive. And when you ask for everything, you get, well, everything. Most days I can tell from the caption of the attachment whether it's a case I should read. Most days, it isn't.

But today the Fifth Circuit redefined the fairly typical contractual liability exclusion in the cyberinsurance context. The fact pattern is common. Retailer hires credit card processor. The processor says, 'ok, we'll take your business, but you'll sign a contract that makes you responsible if anything goes wrong.' The retailer has no choice because you need a processor and they all use the same liability shifting language in their contracts. Then the data breach...

Following the breach, the Payment Card Industry (PCI) comes down on the processor with considerable fines and enhanced security requirements. The processor passes both along to the retailer. The retailer is in the hole, big time.

But we have insurance for this, right?

Most policies still contain language like this: "This insurance does not apply to... 'Loss' on account of any 'Claim' made against any 'Insured' directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. However, this exclusion does not apply to your liability that would have attached in the absence of such contract of agreement."

The District Court construed the processor's demands against Spec's as based entirely on Spec's contractual indemnification requirement contained in its payment card processing agreement. And that is in fact one way to skin a cat. No coverage.

The Fifth Circuit reversed. It reasoned that the second sentence of the exclusion opened the door for the Court to consider other theories of liability for the same asserted damages. While contractual indemnification was one means by which the processor could attempt to collect damages caused by PCI fines and enhanced security requirements, the Fifth Circuit was not convinced that it is the only way. The

Court noted that the processor's demand letters also noted alleged failures by Spec's to meet mandated PCI security protocols, a failure that, in this day and age, could also be deemed ordinary "negligence."

That's the real rub. We all agree that data security must be prioritized, and that lapses must have consequences. We are still grappling, however, with the logistics. Courts have reached widely varying conclusions when evaluating contractual and tort theories of liability, and governmental oversight via statutory and regulatory standards is in its infancy. So, when considering whether any other theory of liability other than breach of contract might attach to data breach related claims against an insured, it would seem to be exceedingly difficult to say no. And the Fifth Circuit just made it a lot more difficult.

Though Spec's is a duty to defend case, which some may argue narrows its application, the contractual liability exclusion found in most cyberinsurance policies was just considerably weakened. Expect to see revised language in response at renewal time.

Posted in: **Legal Developments** and **Policy Terms**

Comments are closed.

[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



JULY 31, 2018

"The New Millennium, and the Old CGL Policies"

By **Jordan M. Rand**

The war to find data breach coverage under commercial general liability (CGL) policies continues to wage. In *St. Paul Fire & Marine Insurance v. Rosen Millennium, Inc. et al.*, filed in March 2017 (M.D. Fla. 6:17-CV-00540), an insurer is seeking a declaration that neither the insured's 2014-15 nor its 2015-16 CGL policy cover data breach costs and a couple million dollars worth of PCI fines.

In 2016, the insured, a hotel, discovered that its payment network had been compromised by malware between September 2014 and February 2016, resulting in the disclosure of customer credit card information. The hotel first tendered to Beazley, its cyber insurer, but Beazley denied coverage on the ground that the "occurrence" happened prior to the applicable retroactive date of the hotel's 2015-16 policy. More on those notorious retro dates [here](#).

The hotel turned to its CGL carrier, St. Paul, which denied coverage for a variety of reasons. Two are especially noteworthy. *First*, St. Paul argues that the ready and known availability of cyber insurance for data breach losses is itself an indication that CGL policies are not intended to cover those losses. *Second*, St. Paul points out that the insured *actually purchased* cyber insurance since 2015-16. Relying on cases holding that courts should construe insurance policies so as *not* to find duplicative coverage, St. Paul argues that the CGL policies must be interpreted so as not to provide coverage for data breach losses because the insured's Beazley policy did provide that coverage.

Eh...

I'd argue that there's no duplicative coverage here. For coverage to be "duplicative," you have to actually have it in at least one other policy. Here, the hotel apparently doesn't. That's why it tendered to St. Paul.

But the more important point is that these relatively new arguments are evidence that it is becoming increasingly difficult to argue for data breach coverage in a CGL policy. From the early 2000's through the Sony litigation in 2015, insureds have sought, and in more than a few cases, found coverage in CGL policies for data breach losses. But as policy language tightens, as ISO and bespoke data breach exclusions are systematically incorporated into non-cyber policies and as the cyber market continues to grow, the CGL coverage argument becomes a far more difficult needle to thread.

Reminder: I don't sell insurance.

Reminder Two: If you have data breach exposure, you probably should buy cyber insurance.

Posted in: **Legal Developments**

Comments are closed.

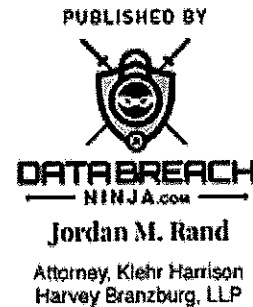
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



OCTOBER 17, 2018

"Voluntary Parting is Not Sweet Sorrow"

By **Jordan M. Rand**

It's (approximately) the ides of National Cybersecurity Awareness Month. Yes, it's a thing. A 15-year old thing. Appropriately, I spent last night at a cybersecurity seminar hosted by Citrin Cooperman (thanks, by the way). It sparked this first of a two-part blog post about the "voluntary parting" exclusion. Get your popcorn ready.

First, the scene. We're at the Union League in Philadelphia. It's kind of dark, because it's always kind of dark in there. Everyone is wearing coats, because everyone has to wear coats there. Despite the lighting and formality (to which I should really be more accustomed in my 11th year as a lawyer), the panel is exceptional. An ethical hacker demonstrates the ease with which he can figure out all of our passwords using software that makes billions of guesses per second. A valuation expert explains the process of quantifying cyber incident losses. Of most interest to me, the general counsel of a sophisticated insurance brokerage offers specific claims insights (no names, of course).

Consistent with the narrative that many of us are hearing, she emphasizes that carriers are by and large responding quickly to, and paying, the majority of cyber claims. So, I ask: "Are there any exclusions that you are seeing create some deviation from that narrative, maybe exclusions that could be addressed during the front-end application process given the tailored nature of cyber policies?"

The answer was surprising. It's not a cyber exclusion that's creating some 'friction.' It's a commercial crime exclusion that insureds may be surprised to see rear its head after what they are sure was a "cyber incident." It's the "voluntary parting" exclusion, and there is nothing sweet about its application.

Take, for example, **Schmidt v. Travelers** (S.D. Ohio 2015). Way back in 2012, in *slightly* more innocent days, a law firm receives an email from a new client in Japan (you know where this is going). The lawyer emails an engagement agreement. The client signs it and emails it back. The lawyer emails a demand letter to a would-be defendant using contact information provided by the client (via email). The defendant emails back, saying, 'sure, we'll pay you the \$378,000 in two equal installments.' The lawyer receives what appears to be a \$189,000 cashier's check from the defendant. The client emails the lawyer instructions to wire him \$141,750, accounting for the lawyer's 25% contingency fee. The lawyer wires the funds. And then finds out that the check was fraudulent.

The lawyer sought coverage under the Computer Fraud endorsement of his business owner's insurance. That coverage applied to losses "resulting directly from the use of any computer to fraudulently cause a transfer of the property" to a third party. The fake client used a computer to fraudulently induce the lawyer to send him money. Square peg, square hole. Right?

Well...

The policy contained a "voluntary parting" exclusion. It excluded coverage for the "voluntary parting with any property by you or anyone else to whom you have entrusted the property." The lawyer argued that the fake-client's fraud precluded a finding that any of his conduct was "voluntary," which is not exactly an off-the wall position. But the court rejected the argument and held that the lawyer voluntarily wired the funds, triggering the exclusion. The money was gone, and there was no insurance for the loss.

These email schemes are now commonplace. The level of sophistication is incredible. Cyber criminals are extraordinarily capable of making fraudulent emails look authentic. There are even increasing instances where criminals use both email *and* the telephone to perpetrate the fraud. Employee training is important, but as in so many other contexts, it is exceedingly difficult to keep up with the rapidly evolving nature of the threat. Risk transfer is essential.

Policyholders may be surprised to learn that not all cyberinsurance policies cover this type of loss, leaving insureds to rely on commercial crime and other similar coverages. Insureds must therefore be wary of "voluntary parting" and similar exclusions, or they must tailor their cyberinsurance to cover email-based fraud.

Tomorrow, I'll tell you about *American Tooling Center, Inc. v. Travelers* (6th Cir. 2018). Spoiler — similar facts, opposite result.

Posted in: **Legal Developments and Policy Terms**

Comments are closed.

[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



OCTOBER 18, 2018

"Part II: Same Email/Wire Scam, Same Carrier, Different Result"

By **Jordan M. Rand**

Yesterday, I wrote about the application of the "voluntary parting" exclusion in *Schmidts v. Travelers*, a 2015 case out of the Southern District of Ohio. If you couldn't tell, I didn't agree with the result.

The Sixth Circuit offered a more reasoned and more recent view of insurance coverage for email/wire scams in *American Tooling Center, Inc. v. Travelers* (July 13, 2018). An American manufacturer received an email purportedly from its Chinese subcontractor. The sub said that the next payment should be wired to a new bank account due to an ongoing audit. The company wired the money. The sub emailed again, saying there was a problem with the account and asking for a new wire to a different account. This happened four times. \$834,000 later, the real sub started asking where its payment was...

The company sought coverage under its Wrap+ business insurance, which contained "computer fraud" coverage. It read: "The Company will pay the Insured for the Insured's direct loss of...Money...directly caused by Computer Fraud." The policy defined "computer fraud" as the "use of any computer to fraudulently cause a transfer of Money..."

Travelers denied the claim, making two arguments relevant to our humble two-part miniseries.

First, Travelers argued that this wasn't computer fraud because the policy "requires a computer to fraudulently cause the transfer. It is not sufficient to simply use a computer and have a transfer that is fraudulent." Basically, Travelers believed that, to trigger coverage, the policy required the malicious actor to gain access to or control an insured's computer to cause a fraudulent wire (as is the case in some cyberinsurance policies). Only, the policy didn't say that. It said "use of any computer to fraudulently cause a transfer of Money." The fake sub used a computer to email fraudulent wiring instructions, which fraudulently caused the company to wire money into the infinite abyss. The Sixth Circuit enforced the policy's clear language, and held that the claim was a covered computer fraud loss.

But...

Travelers also argued that the policy's "voluntary parting" exclusion applied. This one read a little differently from the exclusion in *Schmidts*, stating: "This Crime Policy will not apply to loss resulting directly or indirectly from the giving or surrendering of Money...in exchange or purchase, whether or not fraudulent, with any other party not in collusion with an Employee." Travelers argued that the insured surrendered the payments (read: voluntarily parted with its cash) for goods it had bought from the sub, thereby triggering the exclusion.

The company argued, somewhat like the insured in *Schmidts* who contended that its payment wasn't "voluntary" because it was induced by fraud, that it didn't make the payment in exchange for anything. It was fraudulently induced to pay an impersonator for nothing. The Sixth Circuit agreed and refused to apply the exclusion.

So what?

So, businesses need coverage for email fraud. If you're going to rely on commercial crime or similar non-cyber coverage, make sure to say so during the application process. If you intend to rely on your cyberinsurance, make sure you select or tailor your coverage appropriately. The coverage is available in cyber lines (as I wrote [here](#)), but it isn't in every cyberinsurance policy. And if you're an underwriter or broker familiar with cyber lines incorporating coverage for email/wire fraud scams, let me know and I'll link to samples on my resources page.

Posted in: **Legal Developments and Policy Terms**

Comments are closed.

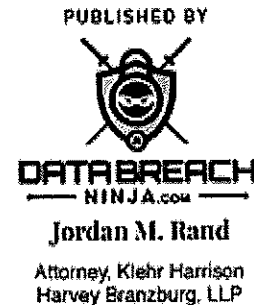
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



DECEMBER 3, 2018

"Common Law Duty to Protect Employee Data Undercuts Contractual Liability Exclusion"

By Jordan M. Rand

Sexy title, I know. Here's the thing – this is a big deal. Particularly for employers, and likely for any entity that collects and stores personal data, the law in Pennsylvania just changed dramatically.

First, a bit of law 101. The "economic loss rule" is a legal concept that recognizes the division of the law into essentially two worlds: tort (*i.e.*, negligence) and contract. Under the rule, no claim exists for negligence that results solely in economic damages without physical injury or property damage. Example: You pay a painter to paint your house. He doesn't. You want to sue for everything, including the emotional distress that comes with living in a home the color of which does not reflect the "real you." But you (probably) can't. Under the economic loss rule, the economic injury suffered when you paid for nothing does not give rise to a negligence claim or to the broader range of damages that may recoverable in tort. You're stuck with a breach of contract claim for your money back and maybe the increased cost of hiring somebody else to paint your house. There are exceptions and nuances, but that's all you need to know for this post.

Courts have reached different conclusions as to whether the economic loss rule bars negligence claims for financial losses caused by data breaches. And some states don't even recognize an independent tort duty to support a negligence claim for a data breach that *is* accompanied by physical damage (say, to your hardware). The United States District Court for the District of Minnesota examined this state-by-state variation in the **Target data breach class action**. The court held that, at least of 2014, negligence claims for data breaches were barred by the economic loss rule in Alaska, California, Illinois, Iowa, Massachusetts and...Pennsylvania. As for class members from the District of Columbia, Georgia, Idaho, New Hampshire and New York, the law was still sufficiently unsettled in those jurisdictions that their negligence claims survived Target's motion to dismiss.

Pennsylvania has officially flipped.

On November 21, 2018, the Pennsylvania Supreme Court held in ***Dittman v. University of Pittsburgh Medical Center*** that employers have a duty to use reasonable care to protect employee data, and that the economic loss rule does not bar tort recovery for financial damages caused by data breaches. *Dittman* is a class action brought on behalf of over 60,000 UPMC employees whose personal information was compromised in a data breach. The employees claim that UPMC failed to use appropriate information security systems to protect their data (social security numbers, birthdates, financial and health

information etc.). The trial court dismissed the class's negligence claims, believing that it is for the legislature and not the courts to establish a new common law duty in the data breach context. The Superior Court affirmed. And the Supreme Court reversed, opening the door for plaintiffs to assert negligence claims arising out of data breaches and seriously expanding the scope of data breach liability in the Commonwealth.

But this is an insurance law blog, isn't it? Yes, and *Dittman* has important consequences in the world of cyberinsurance.

You may recall the contractual liability exclusion, and how excited I was when the Fifth Circuit drew a roadmap around it in the *Spec's* case. Most cyberinsurance policies contain language like this: "This insurance does not apply to... 'Loss' on account of any 'Claim' made against any 'Insured' directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. *However, this exclusion does not apply to your liability that would have attached in the absence of such contract of agreement.*"

Before *Dittman*, insurers could have argued that employee data is collected and maintained pursuant to the contract of employment, the employee handbook or any of the arguably contractual forms routinely filled out by employees during the on-boarding process. Application of the contractual liability exclusion would have likely barred coverage for an employee class action suit like the one in *Dittman*, as there was not yet a clear indication that liability "would have attached in the absence of such contract."

Dittman, however, makes clear that irrespective of what all that paper says, employers have an independent duty to protect employee data, and the economic loss doctrine is no shield to liability if employers fail to do so. The Court explained: "Employees have asserted that UPMC breached its common law duty to act with reasonable care in collecting and storing their personal and financial information on its computer systems. *As this legal duty exists independently from any contractual obligations between the parties*, the economic loss doctrine does not bar Employees' claim." This language likely renders the contractual liability exclusion inapplicable in this context.

Dittman, on the heels of *Spec's* and other cases across the country, reflects a trend of Courts adapting traditional legal frameworks to create, rather than foreclose, liability in the data breach context. As courts define the contours of data breach liability, in both the tort and contract worlds, these decisions will have profound impacts on cyberinsurance coverage issues. For employers that have not yet purchased coverage, *Dittman* warrants a call to your broker. For any entity that already has coverage, *Dittman* is the most recent example of the need to examine evolving laws and liabilities at renewal time.

Posted in: **Legal Developments and Policy Terms**

Comments are closed.

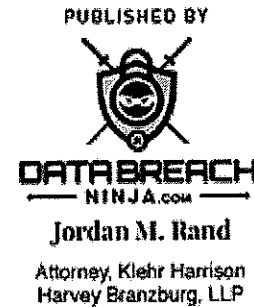
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



JANUARY 2, 2019

"My Least Favorite Exclusion Challenged by Milk's Favorite Cookie"

By **Jordan M. Rand**

Welcome back. Unless you never left, in which case you're probably having a smoother morning than I am. If you're reading this, we're both having better mornings than Mondelez International, Inc. had on June 27, 2017, when the company was hit by the NotPetya attack that rocked pretty much the whole world. Think you never heard of Mondelez? It's the snack food mega company that makes Ritz crackers, Cadbury chocolates and milk's and my favorite cookie – the Oreo.

Refresher on NotPetya – most (including the CIA) believe this attack was propagated by the Russian military against Ukraine, where it is estimated that 50-80% of damage occurred. Many believe that the spread of this malware – the fastest ever as of the time of the attack – to multinational and US corporations was not even intentional. That didn't stop it from causing an estimated \$10 billion in damages to hospitals, banks, shipping companies and others worldwide.

Mondelez, though, has a Zurich insurance policy that specifically covers "physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the malicious introduction of machine code or instruction." When NotPetya hit Mondelez, it permanently destroyed 1,700 servers and 24,000 computers. Mondelez claims that it lost over \$100 million in the form of property damage, commercial supply and distribution disruptions, unfulfilled customer orders and reduced margins. Mondelez tendered a claim to Zurich, and Zurich wasn't exactly sure what to do.

This is what everyone was afraid of, **including me**. The cyberinsurance market has been growing at an exponential rate, but underwriting data is relatively limited compared to other risks and the consequences of an incident like NotPetya are potentially more substantial than any risk ever underwritten. What happens when carriers sell millions, or even billions, of dollars of coverage and then the whole world suffers a giant cyber incident at one time?

Initially, Zurich denied coverage on the sole basis of an 'act of war exclusion,' which I've previously called into question in the context of any cyberinsurance policy [here](#). Zurich took the position that because the Russian military is believed to have launched NotPetya, the incident was a "hostile or warlike action" for which coverage is excluded. Then Zurich allegedly changed its mind, offering to front \$10 million in coverage while reserving its rights. Then Zurich refused to pay anything and issued a second denial of coverage letter asserting of myriad of new grounds to deny coverage. Not great facts for a carrier in any coverage litigation.

Certainly not in this context. The reasonable expectations doctrine may not be at the forefront of every coverage opinion, but I've always believed that Courts try to employ it even if by another, and sometimes completely unrecognizable, name. The doctrine simply requires the insurer to provide an insured with the coverage that the insured reasonably believed it had purchased. Here, Mondelez recognized the severity of the cyber threat faced by large corporations and it had coverage in place. It's probably reasonable to believe that this coverage applies to one of the most significant cyber incidents ever. And as to Mondelez, it would also be reasonable to believe that the attack was not an act of war for at least three reasons: (1) everyone loves Oreos; (2) there may never be definitive proof as to who or what launched the attack and for what purpose, all of which will be Zurich's burden to prove; and (3) even if we accept that this was an attack by Russia against Ukraine, it doesn't even appear to be an attack on the United States, where many believe the consequences were wholly unintended — I haven't looked, but I'm hard-pressed to believe any carrier has ever excluded coverage on the grounds of an unintentional act of war.

This case is likely not the only of its kind in the wake of NotPetya, and its predecessor, WannaCry. Coverage issues presented by these attacks highlight an important potential vulnerability in the cyber market. As attacks increase in scope and effectiveness, it becomes more likely that many insureds will simultaneously suffer significant damages. In this first round of coverage disputes concerning broad-scale attacks, it remains to be seen whether carriers can and will provide the coverage that customers reasonably believed they were buying. In the mean time, make sure to specifically address coverage for large-scale attacks with your broker when buying or renewing coverage. There are likely a number of ways to address these issues, and if there is not an available insurance solution for your particular circumstance, you'd rather find that out upfront than after a potentially company-crippling cyber attack.

Mondelez has filed suit in the Cook County Illinois Circuit Court, Docket No. 2018L011008. Here's Mondelez's **complaint**. Zurich has yet to respond.

Posted in: **Legal Developments and Policy Terms**

Comments are closed.

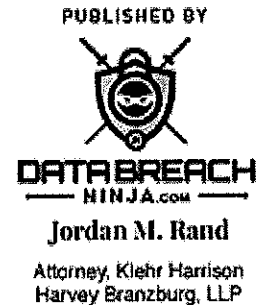
[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



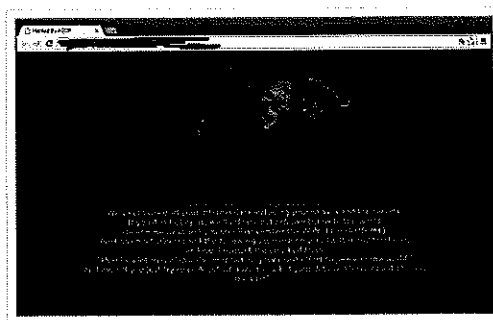
MARCH 28, 2019

"A Tale of Two Carriers – Disparate Views of War/Terrorism Exclusion"

By **Jordan M. Rand**

In January, I offered my view on Zurich's invocation of an 'act of war' exclusion to deny coverage for Mondelez International's losses caused by NotPetya. And made a funny joke about Oreos in the process. You're welcome. More recently, I was interviewed by Matt Fleischer-Black for **CyberInsecurity News** on the same subject, and Matt suggested that his research revealed that Sony's claims were covered by AIG following the 2014 'The Interview' hack. That got me thinking – if AIG covered Sony's losses, is there a difference between Sony's AIG policy and Mondelez's Zurich policy?

Sony reportedly had an AIG CyberEdge policy in place when the "Guardians of Peace" hacked into Sony's network in November 2014. The GOP locked employees computers with a very scary image and threatened to release Sony's data about unreleased movies and confidential business issues. They also threatened "9-11 style" attacks at theatres that showed Sony's "The Interview," a comedy about two reporters sent to assassinate North Korean Supreme Leader Kim Jong Un. The CIA identified the GOP as North Korean state actors, and President Obama enhanced sanctions against North Korea.



I don't have Sony's actual AIG policy. I did, however, find a **sample AIG CyberEdge policy** that would have been in use during Sony's April 2014 -April 2015 policy term. Like Mondelez's Zurich policy, it contains an 'Act of War Exclusion.' The AIG policy bars coverage "arising out of... war, invasion, military action...political disturbance, civil commotion, riot, martial law, civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power..."

Did the act of war exclusion bar coverage for a reportedly North Korean cyber attack that threatened "9-11 style" violence in retaliation for a movie about the assassination of its most powerful political leader? Nope. Sony reported that AIG covered its claim, which some estimate approached \$100 million. President Obama agreed that the GOP hack was not an "act of war." "I don't think it was an act of war," he told CNN. "I think it was an act of cyber vandalism that was very costly, very expensive."

"Cyber vandalism." New words. What do they mean? And what's the difference between "cyber vandalism" and "cyber terrorism," or actual terrorism?

Zurich apparently does not believe that there is any difference. The FBI believes that the Russian military launched NotPetya as an act of aggression against Ukraine. Its propagation across hemispheres and the concomitant billions of dollars of global damages was, well, a happy accident. Certainly, 'The Interview Act' seems *closer* to an act of war or terror as we've historically understood that language than does the NotPetya event that had no political motivations or threats of physical violence as against the United States. And if "cyber vandalism" is a new risk entirely, one not barred by traditional act of war exclusions, NotPetya seems like a good place to start defining its scope.

AIG's coverage position may not be rooted *solely* in a different interpretation of the exclusion. 'The Interview Hack' involved one claim. NotPetya affected thousands of American companies. So, an economic analysis, at least in part, may be driving Zurich to use Mondelez as a test case. Absent settlement, the case is poised to make important precedent. Looking at how Zurich, AIG and other carriers have interpreted comparable exclusions under similar circumstances – thereby establishing a "custom and usage" – should be a significant part of the analysis. Verizon **reported** that nation state driven cyber events comprised 12% of compromises in 2018, and I've seen estimates as high as 50% of breaches as attributable to nation state actors. If nation states are this substantial a threat actor, and if Zurich is permitted to deny coverage based on the act of war/terror exclusion, many insureds will have purchased significantly less valuable coverage than they had believed. This would be precisely the narrative that the cyber market has been trying to avoid as premiums reach as estimated \$5 billion annually.

So, as De La Soul once said, the "stakes is high."

Posted in: **Policy Terms**

Comments are closed.

[« Previous](#) | [Home](#) |

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

Contact Us Now: (215) 569-3024

Cyberinsurance Law Blog



MAY 8, 2019

"Still Not Down with BEC"

By **Jordan M. Rand**

In April 2016, I **highlighted** insurance issues related to business enterprise compromises, or BECs. Yesterday, I had the privilege of presenting on the topic to the Central Jersey Chapter of the Institute of Internal Auditors at its Annual Fraud Conference (thanks to **Frank Pina** at **Mercadian** for the invite).

Since I last wrote about the subject, the FBI has determined that BECs, also known as CEO fraud, social engineering and spoofing, are among the most costly forms of cyber-crime. Refresher: the FBI defines a BEC as a "sophisticated scam targeting both businesses and individuals performing wire transfer payments...[that] is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer engineering techniques to conduct unauthorized transfers of funds." Common examples of BECs are e-mails that appear to come from a CEO or CFO directing an employee to pay a fake vendor and scammers posing as title insurance representatives sending last-minute changes in wiring instructions to real estate purchasers.

Between 2013 and 2018, BECs accounted for over \$12.5 billion in *reported* losses globally. I say *reported* because the FBI's data set is limited to self-reported information received through its Internet Complaint Center, or IC3. Many victims of this type of fraud likely do not report it to the FBI for a multitude of reasons. Of these losses, there have been 41,058 incidents in the United States accounting for nearly \$3 billion in losses. This figure represents more than half of fraud-related losses reported to the FBI during this -five-year period.

So, what are you going to do about? Yes, you. In preparing for my presentation, I learned of the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG). This group is composed of FBI and other law enforcement personnel, regulators and government agencies and private companies and citizens. Started in 2015, it's now the largest global industry association of its kind. The group combats internet abuse and fraud through position papers, training and, most interestingly, setting traps that lead to the arrests of BEC scammers. M3AAWG does this by sending its own socially engineered e-mails to suspected BEC perpetrators to obtain information about what they've done, where they've done it and, critically, where they are. This process has led to over 100 arrests.

I typically focus on transferring risk, but groups like M3AAWG are proactively attacking the attackers. The hunters are becoming the hunted. And I love it. Yes, companies should ensure that they have appropriate risk transfer mechanisms in place, and they should constantly monitor and invest in their front-line security

infrastructure. But maybe you should also consider joining the militia. To find out more about joining M3AAWG, click [here](#) (no, this is not a trick).

Posted in: **News and Policy**

Comments are closed.

[« Previous](#) | [Home](#)

Jordan M. Rand
Klehr Harrison Harvey Branzburg, LLP
1835 Market St #1400
Philadelphia, PA 19103
jrand@klehr.com
Phone: 215-569-3024
Fax: 215-568-6603

Copyright © 2017 – 2019, Jordan M. Rand
JUSTIA Law Firm Blog Design

895 F.3d 455
United States Court of Appeals, Sixth Circuit.

AMERICAN TOOLING CENTER, INC.,
Plaintiff-Appellant,

v.

TRAVELERS CASUALTY AND SURETY
COMPANY OF AMERICA, Defendant-Appellee.

No. 17-2014

|
Argued: May 2, 2018

|
Decided and Filed: July 13, 2018

|
Rehearing En Banc Denied August 28, 2018

Synopsis

Background: Insured brought action challenging insurer's denial of claim under its business insurance policy. The United States District Court for the Eastern District of Michigan, No. 5:16-cv-12108, John Corbett O'Meara, J., 2017 WL 3263356, entered summary judgment in insurer's favor, and insured appealed.

Holdings: The Court of Appeals, Karen Nelson Moore, Circuit Judge, held that:

[1] insured suffered "direct" loss when it mistakenly transferred funds intended to Chinese seller to impersonator;

[2] impersonator's fraudulent scheme to cause insured to transfer funds intended for seller to its own accounts constituted "computer fraud";

[3] insured's loss was directly caused by impersonator's computer fraud;

[4] insured's claim did not fall within scope of exclusion for losses "resulting directly or indirectly from the giving or surrendering of Money, Securities or Other Property in any exchange or purchase, whether or not fraudulent, with any other party not in collusion with an Employee";

[5] insured's claim did not fall within scope of exclusion for "loss or damages resulting directly or indirectly from the input of Electronic Data"; and

[6] insured's claim did not fall within scope of exclusion for "loss resulting directly or indirectly from forged, altered or fraudulent documents or written instruments used as source documentation in the preparation of Electronic Data."

Reversed and remanded.

West Headnotes (14)

[1] Federal Courts

Summary judgment

Court of Appeals reviews de novo district court's grant of summary judgment. Fed. R. Civ. P. 56(a).

Cases that cite this headnote

[2] Federal Courts

Summary judgment

In reviewing district court's grant of summary judgment, Court of Appeals reviews all facts in light that is most favorable to, and draw all reasonable inferences in favor of, nonmoving party. Fed. R. Civ. P. 56(a).

Cases that cite this headnote

[3] Insurance

Burden of proof

Under Michigan law, insured has burden of proving coverage.

Cases that cite this headnote

[4]

Insurance

⚡Burden of proof

Under Michigan law, if insured demonstrates that policy provides coverage, then insurer has burden of showing that exclusion provision precludes coverage.

Cases that cite this headnote

Cases that cite this headnote

[5]

Insurance

⚡Application of rules of contract construction

Michigan courts interpret **insurance** policy's terms in accordance with Michigan's well-established principles of contract construction.

Cases that cite this headnote

[8]

Insurance

⚡Risks or Losses Covered and Exclusions

Under Michigan law, insured buyer suffered "direct" loss when it mistakenly transferred funds intended to Chinese seller to impersonator, for purposes of determining its insurer's duty to indemnify buyer for its loss under computer fraud provision of its business **insurance** policy, even though buyer contractually owed that money to seller, and they later agreed to spread loss between them.

Cases that cite this headnote

[6]

Insurance

⚡Plain, ordinary or popular sense of language

Under Michigan law, if **insurance** policy does not define relevant term, reviewing courts must interpret terms of contract in accordance with their commonly used meanings.

Cases that cite this headnote

[9]

Insurance

⚡Theft or Burglary

Under Michigan law, third party's fraudulent scheme to cause insured buyer to transfer funds intended for Chinese seller to its own accounts constituted "computer fraud" under buyer's business **insurance** policy, despite insurer's contention that it was not sufficient to simply use computer and have transfer that was fraudulent, where third party sent buyer fraudulent e-mails using computer and these e-mails fraudulently caused buyer to transfer money to third party.

Cases that cite this headnote

[7]

Federal Courts

⚡Highest court

Federal Courts

⚡Inferior courts

When sitting in diversity jurisdiction, federal court must follow controlling decision of highest state court, but if state's highest court has not spoken on precise issue, federal court must follow state appellate court's decision, published or unpublished, unless it is convinced by other persuasive data that state's highest court would decide otherwise.

[10]

Insurance

⚡Theft or Burglary

Under Michigan law, insured buyer's loss arising from its mistaken transfer of funds to third party impersonating Chinese seller was directly caused by impersonator's computer fraud, and thus insurer had duty to indemnify buyer for its loss under its business **insurance** policy's computer fraud coverage, where buyer

received fraudulent e-mail from impersonator claiming to be seller, buyer's employees then conducted series of internal actions, all induced by fraudulent e-mail, which led to transfer of money to impersonator, and loss occurred when buyer transferred money.

Cases that cite this headnote

[11]

Insurance

⚡Exclusions, exceptions or limitations

Insurance

⚡Exclusions and limitations in general

Under Michigan law, exclusions in insurance policies are strictly construed in insured's favor, although clear and specific exclusions must be enforced.

Cases that cite this headnote

[12]

Insurance

⚡Voluntary parting with possession

Under Michigan law, insured buyer's claim for losses it incurred when it mistakenly transferred funds to third party impersonating Chinese seller did not fall within scope of exclusion in its business insurance policy for losses "resulting directly or indirectly from the giving or surrendering of Money, Securities or Other Property in any exchange or purchase, whether or not fraudulent, with any other party not in collusion with an Employee," where buyer did not give or surrender money to impersonator in "exchange or purchase."

Cases that cite this headnote

[13]

Insurance

⚡Risks or Losses Covered and Exclusions

Under Michigan law, insured buyer's employee's manual entry of imposter's banking

details into banking portal was not "electronic data," for purposes of exclusion in business insurance policy for "loss or damages resulting directly or indirectly from the input of Electronic Data," where policy's definition of "Electronic Data" excluded "instructions or directions to a Computer System."

Cases that cite this headnote

[14]

Insurance

⚡Risks or Losses Covered and Exclusions

Under Michigan law, insured buyer's employee's manual entry of imposter's banking details into banking portal was not "electronic data," for purposes of exclusion in business insurance policy for "loss resulting directly or indirectly from forged, altered or fraudulent documents or written instruments used as source documentation in the preparation of Electronic Data," where policy's definition of "Electronic Data" excluded "instructions or directions to a Computer System."

Cases that cite this headnote

*457 Appeal from the United States District Court for the Eastern District of Michigan at Ann Arbor. No. 5:16-cv-12108—John Corbett O'Meara, District Judge.

Attorneys and Law Firms

ARGUED: Douglas Young, WILSON YOUNG PLC, Southfield, Michigan, for Appellant. Joel T. Wiegert, MEAGHER & GEER, P.L.L.P., Minneapolis, Minnesota, for Appellee. ON BRIEF: Douglas Young, WILSON YOUNG PLC, Southfield, Michigan, for Appellant. Joel T. Wiegert, Anthony J. Alt, MEAGHER & GEER, P.L.L.P., Minneapolis, Minnesota, for Appellee.

Before: MOORE, CLAY, and KETHLEDGE, Circuit Judges.

OPINION

KAREN NELSON MOORE, Circuit Judge.

The plaintiff, American Tooling Center, Inc. (“ATC”), is a Michigan company that subcontracts some of its manufacturing work to a vendor in China. Between October 1, 2014 and October 1, 2015, it was insured by the defendant, Travelers Casualty and Surety Company of America (“Travelers”). During this time period, ATC received a series of emails, purportedly from its Chinese vendor, claiming that the vendor had changed its bank accounts and ATC should wire transfer its payments to these new accounts. After ATC had transferred approximately \$834,000, it learned that the emails were fraudulent and had been sent by a wrongdoer impersonating its Chinese vendor. ATC therefore sought coverage for its loss under its “Wrap+” business insurance policy (“the Policy”), which it had purchased from Travelers. Travelers denied the claim. ATC sued for breach of contract, both parties moved for summary judgment, and the district court granted summary judgment to Travelers. For the following reasons, we **REVERSE** the district court’s grant of summary judgment to Travelers, grant summary judgment to ATC, and **REMAND** for further proceedings consistent with this opinion.

I. FACTS AND PROCEDURE

ATC is a tool and die manufacturer in Michigan that produces stamping dies for the automotive industry. R. 21-3 (Gizinski Dep. at 8) (Page ID #286). The company outsources some of its manufacturing orders. *Id.* at 19 (Page ID #289). Shanghai YiFeng Automotive Die Manufacture Co., Ltd. (“YiFeng”), a Chinese company, is one of ATC’s vendors. *Id.* ATC pays its vendors in four separate payments, based on the manufacturing progress of the order. *Id.* at 36–42 (Page ID #293–95). In order to be paid for the work it has done, YiFeng emails ATC invoices. *Id.* at 45 (Page ID #296). After receiving an invoice *458 from YiFeng, ATC goes through a multi-step process before it will wire the money to YiFeng.

First, ATC employees verify that YiFeng has completed the necessary steps required by the payment schedule for the next payment. *Id.* at 48 (Page ID #296). Each week, ATC’s Vice President and Treasurer, Gary Gizinski,

reviews a physical spreadsheet of the outstanding accounts payable and determines which bills need to be paid that week. R. 21-3 (Gizinski Dep. at 59–61) (Page ID #299–300). ATC pays YiFeng and its other international vendors via wire transfer. *Id.* at 62 (Page ID #300). To initiate a wire transfer, Gizinski signs into a banking portal using software on his computer. *Id.* at 70 (Page ID #302). He manually enters the payee’s name, banking information, and the amount to be wired. *Id.* at 69, 140 (Page ID #302, 319). After Gizinski submits the wire transfer request, ATC’s Assistant Comptroller must log into the banking portal using his computer to approve it. *Id.* at 72 (Page ID #302).

This is the procedure for paying invoices that ATC employees followed in the spring of 2015. On March 18, 2015, Gizinski emailed YiFeng employee Jessie Chen requesting that Chen provide ATC all outstanding invoices. R. 21-4 (Proof of Loss at 23) (Page ID #351). An unidentified third party, through means unknown, intercepted this email. *Id.* at 24 (Page ID #352). This third party, impersonating Chen, then began a correspondence with Gizinski about the outstanding invoices. *See, e.g., id.* at 39–40 (Page ID #367–68). On March 27, 2015, the impersonator emailed Gizinski and claimed that, due to an audit, ATC should wire its payments to a different account from usual. *Id.* at 45 (Page ID #373). YiFeng had previously (and legitimately) informed ATC it had changed its banking details, and ATC had no process for verifying the changed information. R. 21-3 (Gizinski Dep. at 114, 117) (Page ID #313–14). Consequently, Gizinski wired the money to the new account. *Id.* at 142 (Page ID #320).

On April 3, the impersonator emailed Gizinski and informed him that “due to some new bank rules in the province,” the previous wire transfer was not credited to its account and therefore it would return the payment. R. 21-4 (Proof of Loss at 63) (Page ID #391). The impersonator requested that Gizinski instead wire the money to a different bank account. *Id.* Gizinski wired the money to this new account on April 8, 2015. R. 23-10 (Apr. 8, 2015 Wire Transfer) (Page ID #736). The impersonator ran this scam two more times and Gizinski wired additional payments of \$1575 and \$482,640.41 on April 9, 2015 and May 8, 2015. R. 21-4 (Proof of Loss at 3) (Page ID #331). When the real YiFeng demanded payment, ATC realized it had wired the money to an imposter. R. 21-3 (Gizinski Dep. at 166) (Page ID #326). ATC paid YiFeng approximately 50% of the outstanding debt, and agreed that the remaining 50% would be contingent on ATC’s insurance claim. *Id.* at 126–27 (Page ID #316).

ATC sought recovery for its loss from Travelers, arguing that it fell within the “Computer Fraud” provision of the Policy, but Travelers denied the claim. R. 21-5 (July 8, 2015 Denial Ltr.) (Page ID #459–61); R. 21-6 (Sept. 16, 2015 Appeal Ltr.) (Page ID #463–67); R. 21-7 (Oct. 23, 2015 Affirming Denial Ltr.) (Page ID #469–71). ATC subsequently sued Travelers for breach of contract. R. 1 (Compl.) (Page ID #1–16). After discovery, both parties moved for summary judgment. R. 21 (Pl. Mot. for Summ. J.) (Page ID #170–98); R. 22 (Def. Mot. for Summ. J.) (Page ID #591–623). The district court granted Travelers summary judgment, holding that *459 ATC’s loss was not covered under the Policy. R. 33 (Dist. Ct. Op. at 7–8) (Page ID #969–70). ATC timely appealed. R. 35 (Notice of Appeal) (Page ID #972–73).

II. ANALYSIS

A. Standard of Review

^[1] ^[2]We review de novo a district court’s grant of summary judgment. *Luna v. Bell*, 887 F.3d 290, 297 (6th Cir. 2018). Summary judgment is proper if the moving party “shows that there is no genuine dispute as to any material fact.” FED. R. CIV. P. 56(a). “For this determination, we review all facts in a light that is most favorable to, and draw all reasonable inferences in favor of, the nonmoving party.” *Byrd v. Tenn. Wine & Spirits Retailers Ass’n*, 883 F.3d 608, 613 (6th Cir. 2018) (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986)).

^[3] ^[4]The parties agree that Michigan law governs the interpretation of the Policy. Appellant Br. at 4; Appellee Br. at 18. Under Michigan law, the insured has the burden of proving coverage. *Pioneer State Mut. Ins. Co. v. Dells*, 301 Mich.App. 368, 836 N.W.2d 257, 263 (2013) (citing *Solomon v. Royal Maccabees Life Ins. Co.*, 243 Mich.App. 375, 622 N.W.2d 101, 103 (2000)). If the insured demonstrates that the policy provides coverage, then the insurer has the burden of showing that an exclusion provision precludes coverage. *Id.* (citing *Heniser v. Frankenmuth Mut. Ins. Co.*, 449 Mich. 155, 534 N.W.2d 502, 510 (1995)).

B. Coverage

ATC argues that its loss is a result of computer fraud, which is a type of computer crime the Policy covers. Appellant Br. at 5. The Policy states:

F. Computer Crime

1. Computer Fraud

The Company will pay the Insured for the Insured’s direct loss of, or direct loss from damage to, **Money, Securities and Other Property** directly caused by **Computer Fraud**.

R. 21-2 (Policy at 27) (Page ID #227) (emphasis in original denoting terms explicitly defined by the Policy). Travelers argues that there is no coverage because: (1) ATC did not suffer a “direct loss”; (2) this is not a case of “Computer Fraud”; (3) the loss was not “directly caused by Computer Fraud.” Each of these arguments fails: ATC’s loss is covered by the Policy.

1. ATC Suffered a “Direct Loss”

ATC and Travelers disagree about whether the three wire transfers of money to the impersonator constitute a “direct loss” of ATC’s money. Appellant Br. at 13–14; Appellee Br. at 15–17. ATC argues that it suffered a direct loss the moment it paid \$834,107.76 to the impersonator, because it no longer had that money in its bank account. Appellant Br. at 13. In contrast, Travelers argues that the loss did not arise when ATC paid the impersonator—because ATC had already contracted with YiFeng to pay that amount of money for the product it had received—but instead the loss arose later, after the fraud was discovered, when ATC agreed to pay YiFeng at least half of the money still owed. Appellee Br. at 15. At issue is what is meant by the word “direct.”

^[5] ^[6]Michigan courts interpret the terms of an insurance policy “in accordance with Michigan’s well-established principles of contract construction.” *Citizens Ins. Co. v. Pro-Seal Serv. Grp., Inc.*, 477 Mich. 75, 730 N.W.2d 682, 685 (2007) (quoting *Henderson v. State Farm Fire & Cas. Co.*, 460 Mich. 348, 596 N.W.2d 190, 193 (1999)). If a policy does not define a relevant term “reviewing courts must interpret *460 the terms of the contract in accordance with their commonly used meanings.” *Id.* at 686 (quoting *Henderson*, 596 N.W.2d at 194).

^[7]The Michigan Supreme Court has not previously analyzed the meaning of the word “direct” in an

insurance policy. But the Michigan Court of Appeals, in an unpublished decision, has done so.¹ In *Acorn Investment Co. v. Michigan Basic Property Insurance Ass'n*, No. 284234, 2009 WL 2952677, at *2 (Mich. Ct. App. Sept. 15, 2009), Michigan's appellate court defined a "direct" loss as one resulting from an " 'immediate' or 'proximate' cause, as distinct from remote or incidental causes." This definition comports with the plain meaning of the word "direct," as evidenced by relevant dictionary definitions. *Id.* at *2 (citing a dictionary "defining 'direct,' in pertinent part, as 'without intermediary agents, conditions, etc.; immediate'"). *Merriam-Webster* defines "direct" as "proceeding from one point to another in time or space without deviation or interruption[;] ... characterized by or giving evidence of a close especially logical, causal, or consequential relationship." *Direct*, MERRIAM-WEBSTER UNABRIDGED, <http://unabridged.merriam-webster.com/unabridged/direct> (last visited June 6, 2018). Similarly, *Black's Law Dictionary* states that direct means: "(Of a thing) straight; undeviating ... immediate." *Direct*, BLACK'S LAW DICTIONARY (10th ed. 2014); see also *Loss—Direct Loss*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A loss that results immediately and proximately from an event.").

Travelers argues that we should reject the definition of "direct" from *Acorn*, and instead utilize a narrower definition articulated by this court in the context of Michigan employee-fidelity bonds. Appellee Br. at 14. In *Tooling, Manufacturing & Technologies Ass'n v. Hartford Fire Insurance Co.*, 693 F.3d 665, 676 (6th Cir. 2012), we stated that "direct is direct." In other words, "direct" means "immediate." See *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 691 F.3d 821, 828 (6th Cir. 2012) (describing the "direct means direct" approach); *Universal Mortg. Corp. v. Württembergische Versicherung AG*, 651 F.3d 759, 761–62 (7th Cir. 2011) (same). Our decision in *Tooling* is entrenched in the jurisprudence of interpreting employee-fidelity bonds, where a split has arisen over the issue of how to define "direct," and the development of the language of these bonds plays an important role in interpreting them. Compare *Tooling, Mfg. & Techs.*, 693 F.3d at 674–75, with *Universal Image Prods., Inc. v. Fed. Ins. Co.*, 475 F. App'x 569, 573 (6th Cir. 2012) (applying the definition of "direct" from *Acorn* to a property-damage insurance policy governed by Michigan law). In *Tooling*, we cited this "unique" context as a reason to distinguish the facts in *Tooling* from *Acorn*. *Id.* at 677. We need not resolve here whether *Tooling* is limited to the context of employee-fidelity bonds or is more broadly applicable because ATC suffered a "direct loss" under either definition—direct as immediate only or direct as

immediate or proximate.

^[8] ATC immediately lost its money when it transferred the approximately \$834,000 to the impersonator; there was no intervening event. *Id.* at *2. Despite Travelers' argument to the contrary, Appellee *461 Br. at 15, the fact that ATC contractually owed that money to YiFeng and the two parties later agreed to spread the loss between them has no bearing on whether this loss was directly suffered by ATC. A simplified analogy demonstrates the weakness of Travelers' logic. Imagine Alex owes Blair five dollars. Alex reaches into her purse and pulls out a five-dollar bill. As she is about to hand Blair the money, Casey runs by and snatches the bill from Alex's fingers. Travelers' theory would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill. This interpretation defies common sense.

2. The Impersonator's Conduct Constitutes "Computer Fraud"

The two parties also contest whether the impersonator's fraudulent scheme constitutes "Computer Fraud." Appellant Br. at 19; Appellee Br. at 19. The Policy specifically defines the term:

E. Computer Fraud means:

The use of any computer to fraudulently cause a transfer of **Money, Securities or Other Property** from inside the **Premises or Financial Institution Premises**:

1. to a person (other than a **Messenger**) outside the **Premises or Financial Institution Premises**; or
2. to a place outside the **Premises or Financial Institution Premises**.

R. 21-2 (Policy at 31) (Page ID #231) (emphasis in original denoting terms explicitly defined by the Policy). Travelers does not contest that there was a transfer of money from ATC's bank (a "Financial Institution Premises") to a person (other than a "Messenger"). Instead, it argues that this definition of "Computer Fraud" requires a computer to "fraudulently cause the transfer. It is not sufficient to simply use a computer and have a transfer that is fraudulent." Appellee Br. at 19.

In support of this argument, Travelers points to an unpublished decision from the Ninth Circuit, which

interpreted this exact provision under California law. Appellee Br. at 19–20. In *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, 656 F. App'x 332, 333 (9th Cir. 2016), our sister circuit “interpret[ed] the phrase ‘fraudulently cause a transfer’ to require an unauthorized transfer of funds.” The Ninth Circuit acknowledged that “Travelers could have drafted this language more narrowly,” but “[b]ecause computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a ‘General Fraud’ Policy.” *Id.*

Pestmaster is distinguishable for multiple reasons, but principally it is distinguishable on its facts. In that case, Pestmaster had hired Priority 1 Resource Group to handle its payroll tax services and granted Priority 1 electronic access to its bank account. *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 13-5039-JFW (MRWx), 2014 WL 3844627, at *1 (C.D. Cal. July 17, 2014), *aff'd in part and rev'd in part*, *Pestmaster Servs., Inc.* 656 F. App'x 332. Priority 1 was then authorized to transfer funds out of Pestmaster's bank account into its own account, and from there it was to pay Pestmaster's payroll taxes. *Id.* The fraud occurred when Priority 1 failed to pay the taxes and kept the money instead. *Id.* at *2. Thus, in *Pestmaster*, everything that occurred using the computer was legitimate and the fraudulent conduct occurred without the use of a computer.

^[9]In contrast, here the impersonator sent ATC fraudulent emails using a computer and these emails fraudulently caused *462 ATC to transfer the money to the impersonator. See, e.g., R. 21-4 (Proof of Loss at 39–40) (Page ID #367–68). And the Policy definition does not require, as Travelers argues, that the fraud “cause any computer to do anything.” Appellee Br. at 20. Travelers' attempt to limit the definition of “Computer Fraud” to hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer is not well-founded. If Travelers had wished to limit the definition of computer fraud to such criminal behavior it could have done so.² Cf. *Citizens Ins. Co.*, 730 N.W.2d at 686 (holding that a contract is construed in favor of the insured if there is an ambiguity). Because Travelers did not do so, the third party's fraudulent scheme in this case constitutes “Computer Fraud” per the Policy's definition.

Computer Fraud”

^[10]ATC must also show that its “direct loss” was “directly caused” by the computer fraud. ATC has met its burden, because the computer fraud was an immediate cause of its loss. *Acorn Inv. Co.*, 2009 WL 2952677, at *2; *Tooling, Mfg. & Techs.*, 693 F.3d at 676.

The chain of events that was precipitated by the fraudulent emails and led to the wire transfers involved multiple internal actions at ATC. After receiving each fraudulent email, ATC verified that YiFeng had completed the tasks required for the next scheduled payment. R. 21-3 (Gizinski Dep. at 48 (Page ID #296)). Gizinski subsequently determined which outstanding invoices to pay, and chose to pay the YiFeng invoice. *Id.* at 59–61 (Page ID #299–300). He then signed into the banking portal and manually entered the fraudulent banking information emailed by the impersonator. *Id.* at 69, 140 (Page ID #302, 319). Finally, after Gizinski submitted the wire transfer, ATC's Assistant Comptroller approved the payment. *Id.* at 72 (Page ID #302). ATC thus suffered its loss immediately after the transfer, which marked the end of the “Computer Fraud” as defined in the policy.

A recent unpublished decision from the Eleventh Circuit provides a helpful counterpoint. In *Interactive Communications International, Inc. v. Great American Insurance Co.*, — F. App'x —, No. 17-11712, 2018 WL 2149769 (11th Cir. May 10, 2018), the Eleventh Circuit analyzed whether, under Georgia law, the insured's loss “resulted directly” from computer fraud. In that case, there was a multi-step, multi-actor process that caused the loss. First, the bad actors manipulated the insured's computer system essentially allowing for a double redemption of pre-paid, reloadable debit cards—this was the computer fraud. *Id.* at —, 2018 WL 2149769 at *4. Second, this fraud induced the insured to transfer the money to its account held by an innocent third-party intermediary. *Id.* Third, the bad actors made a purchase using the debit cards. *Id.* at —, 2018 WL 2149769 at *5. Fourth, the third party deducted the amount of the purchase from the insured's account. *Id.* Even though the insured transferred the money at step two, it retained control over the money until after the fourth step. Indeed, “[o]n one particular occasion, after identifying fraud associated with \$1.9 million *463 in duplicate redemptions by some debit card holders,” the insured unilaterally froze those cards. *Id.* Thus, the computer fraud occurred at step one; but “the point of no return” after which the money had left the control of the insured occurred not at step two—when it transferred the money to the third-party intermediary—but after step four. *Id.* The Eleventh Circuit concluded that “[t]he lack

3. ATC's “Direct Loss” Was “Directly Caused by

of [temporal] immediacy—and the presence of intermediate steps, acts, and actors—” meant “that the loss did not ‘result[] directly’ ” from the computer fraud. *Id.* (third alteration in original). In reaching this decision, the Eleventh Circuit applied a “direct means immediate” definition, as opposed to the “direct means immediate or proximate” definition.⁷ Applying the narrower definition, the Eleventh Circuit suggested that if the “point of no return” was at step two—when the insured transferred the money—this would have been a direct result of the computer fraud at step one. *Id.*

This is what occurred in this case, when framed at the same level of generality as the Eleventh Circuit used. ATC received the fraudulent email at step one. ATC employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was “the point of no return,” because the loss occurred once ATC transferred the money in response to the fraudulent emails. Thus, the computer fraud “directly caused” ATC’s “direct loss.”

C. Exclusions

^[11]Travelers argues that, regardless of the Policy’s coverage, three exclusion provisions apply: G, H, and R. Travelers made this argument in front of the district court, R. 22 (Def. Mot. for Summ. J. at 20–23) (Page ID #618–20), but the district court did not reach it. Under Michigan law, exclusions are “strictly construed in favor of the insured,” although “clear and specific exclusions must be enforced.” *Hunt v. Drielick*, 496 Mich. 366, 852 N.W.2d 562, 565–66 (2014) (brackets omitted) (first quoting *Auto-Owners Ins. Co. v. Churchman*, 440 Mich. 560, 489 N.W.2d 431, 434 (1992); and then quoting *Group Ins. Co. of Mich. v. Czopek*, 440 Mich. 590, 489 N.W.2d 444, 447 (1992)). None of the exclusions asserted by Travelers preclude coverage in this case.

1. Exclusion R

Travelers first argues that Exclusion R applies. Appellee Br. at 33–34. This provision states, in pertinent part:

This **Crime Policy** will not apply to loss resulting directly or indirectly from the giving or surrendering of **Money, Securities**

or **Other Property** in any exchange or purchase, whether or not fraudulent, with any other party not in collusion with an **Employee**
....

R. 21-2 (Policy at 39) (Page ID #239) (emphasis in original denoting terms explicitly defined by the Policy). Travelers contends that Exclusion R applies because ATC transferred the money to the impersonator, believing it to be YiFeng, in exchange for the goods it had received from the vendor. Appellee Br. at 34. ATC correctly points out that it did not transfer the money to the impersonator in exchange for anything from the impersonator, and therefore the fraudulent transfer does not fall within this exclusion provision. Appellant Reply Br. at 9.

*464 ^[12]We have previously analyzed a similar exclusion provision, under Tennessee law, which included the language “giving or surrendering of Money or Securities in any exchange or purchase.” *Harrah’s Entm’t, Inc. v. Ace Am. Ins. Co.*, 100 F. App’x 387, 391 (6th Cir. 2004). In that case, we noted that the provision was “loosely worded” and potentially ambiguous, and therefore should be construed against the drafter. *Id.*; see also *Hunt*, 852 N.W.2d at 565–66. Construing this provision in favor of ATC and against its drafter, Travelers, we hold that ATC’s wire transfers to the impersonator do not fall within Exclusion R, because ATC did not give or surrender money to the impersonator in an “exchange or purchase.”

2. Exclusion G

Travelers next argues that Exclusion G applies to this situation. Appellee Br. at 35–36. The relevant section of Exclusion G states:

This **Crime Policy** will not apply to loss or damages resulting directly or indirectly from the input of **Electronic Data** by a natural person having the authority to enter the **Insured’s Computer System**
....

R. 21-2 (Policy at 39) (Page ID #238) (emphasis in original denoting terms explicitly defined by the Policy). “Electronic Data” is defined as “facts or information converted to a form: (1) usable in a **Computer System**; (2) that does not provide instructions or directions to a

Computer System; or (3) that is stored on electronic processing media for use by a **Computer Program**.” *Id.* at 32 (Page ID #232) (emphasis in original denoting terms explicitly defined by the Policy). A “Computer System” is “a computer and all input, output, processing, storage and communication facilities and equipment that are connected to such a device and that the [sic] operating system or application software used by the **Insured** are under the direct operational control of the **Insured**....” *Id.* at 31 (Page ID #231) (emphasis in original denoting terms explicitly defined by the Policy).

^[13]Travelers summarily states that, when Gizinski manually entered the impersonator’s name, banking information, and the amount to be wired into the banking portal, he was inputting “Electronic Data.” Appellee Br. at 35–36. But the definition of “Electronic Data” excludes “instructions or directions to a **Computer System**.” R. 21-2 (Policy at 32) (Page ID #232) (emphasis in original denoting terms explicitly defined by the Policy). Strictly construed against Travelers, *Hunt*, 852 N.W.2d at 565–66, Gizinski’s manual entry of the imposter’s banking details was not “Electronic Data.” The physical pressing of the keyboard and mouse sent instructions to the computer to display specific values. *Computer*, *ENCYCLOPÆDIA BRITANNICA*, <https://academic.eb.com/levels/collegiate/article/computer/117728> (last visited June 7, 2018). These values combined to form “instructions or directions,” R. 21-2 (Policy at 32) (Page ID #232), to act in a specific manner; i.e. to transmit the entered values from ATC to the banking portal via the “communication facilities” of the “Computer System,” *id.* at 31 (Page ID #231).

Arguably, this interpretation the Policy’s definition of “Electronic Data” is narrower than our ordinary understanding of electronic data. *Cf. Citizens Ins. Co.*, 730 N.W.2d at 686 (holding that courts should look to the common understanding of a word when it is not defined in the policy). But Travelers chose to define this phrase, as opposed to rely on its ordinary meaning, and it did so with the broad exception that “facts or information” that “provide instructions or directions” are *not* “Electronic Data.” R. 21-2 (Policy at 32) (Page *465 ID #232). Ambiguities in an insurance contract are construed in favor of the insured, *Citizens Ins. Co.*, 730 N.W.2d at 686, and exclusion provisions are strictly construed against the insurer, *Hunt*, 852 N.W.2d at 565–66. Thus, Exclusion G is inapplicable in this case because the fraudulent bank-routing instructions do not constitute “Electronic

Data” as defined by Travelers.

3. Exclusion H

^[14]Finally, Travelers argues that ATC is not covered by the Policy because of Exclusion H, which states:

This **Crime Policy** will not apply to loss resulting directly or indirectly from forged, altered or fraudulent documents or written instruments used as source documentation in the preparation of **Electronic Data**

R. 21-2 (Policy at 38) (Page ID #238) (emphasis in original denoting terms explicitly defined by the Policy). Travelers contends that the impersonator’s **emails** constitute “fraudulent documents” and that Gizinski relied upon those **emails** when entering the information into the banking portal to initiate the wire transfer. Appellee Br. at 37. For the reasons stated in Section II.C.2, *supra*, Gizinski’s entries into the banking portal do not constitute “Electronic Data” as defined by the Policy. Consequently, Exclusion H is inapplicable and does not preclude coverage.

III. CONCLUSION

For the foregoing reasons, we hold that ATC’s loss is covered by the Policy and none of the asserted Policy exclusions apply. Thus, we **REVERSE** the district court’s grant of summary judgment to Travelers, grant summary judgment to ATC, and **REMAND** for further proceedings consistent with this opinion.

All Citations

895 F.3d 455

Footnotes


¹ When sitting in diversity jurisdiction, this court must follow the controlling decision of the highest state court. But if the “state’s highest court has not spoken on a precise issue,” this court must follow a decision of the state appellate court,

published or unpublished, "unless it is convinced by other persuasive data that the highest court of the state would decide otherwise." *Ziegler v. IBP Hog Mkt., Inc.*, 249 F.3d 509, 517 (6th Cir. 2001) (quoting *Puckett v. Tenn. Eastman Co.*, 889 F.2d 1481, 1485 (6th Cir. 1989)).

- 2 There are **insurance** policies that define computer fraud much more narrowly. See, e.g., *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 25 N.Y.3d 675, 37 N.E.3d 78, 79 (2015) (describing a policy defining "Computer Systems Fraud" as "Loss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program into, or (2) change of Electronic Data or Computer Program within the Insured's proprietary Computer System").
- 3 The Eleventh Circuit also noted that the difference between these two definitions "may be smaller than it appears." *Interactive Commc'ns Int'l, Inc.*, — F. App'x at — n.2, 2018 WL 2149769, at *3 n.2.

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.

 KeyCite Yellow Flag - Negative Treatment
Declined to Follow by Medidata Solutions, Inc. v. Federal Insurance Co., S.D.N.Y., July 21, 2017

662 Fed.Appx. 252

This case was not selected for publication in West's Federal Reporter.

See Fed. Rule of Appellate Procedure 32.1 generally governing citation of judicial decisions issued on or after Jan. 1, 2007. See also U.S.Ct. of App. 5th Cir.

Rules 28.7 and 47.5.

United States Court of Appeals, Fifth Circuit.

APACHE CORPORATION, Plaintiff–Appellee
Cross–Appellant

v.

GREAT AMERICAN INSURANCE COMPANY,
Defendant–Appellant Cross–Appellee

No. 15–20499

|

Date Filed: 10/18/2016

Synopsis

Background: Insured filed state court suit against insurer, challenging denial of claim under crime-protection insurance policy, for approximately \$2.4 million loss sustained from criminals defrauding insured, partly by using e-mail from incorrect website address for vendor instructing insured to use new bank account for making payments to vendor, which insured followed after flawed follow-up investigation and made authorized payments for vendor's legitimate invoices to criminals' fraudulent bank account. Following removal, the United States District Court for the Southern District of Texas, Alfred H. Bennett, J., 2015 WL 7709584, granted insured summary judgment. Insurer appealed.

[Holding:] The Court of Appeals held that loss was not covered under policy's computer fraud provision.

Vacated and judgment rendered for insurer.

West Headnotes (1)

[1] Insurance

☛ Theft or Burglary

Under Texas law, as predicted by Court of Appeals, insured's loss from being defrauded by criminals using e-mail from incorrect website address for vendor, instructing insured to use new bank account for making payments to vendor, which insured followed after flawed investigation and made authorized payments for vendor's legitimate invoices to criminals' bank account, was not covered occurrence "resulting directly from the use of any computer to fraudulently cause a transfer" of funds, within meaning of computer fraud provision of crime-protection policy, since e-mail was part of scheme but merely incidental to authorized transfer of money, as computer use was but one step in insured's multi-step flawed process that ended in making authorized very large invoice payments to fraudulent account.

7 Cases that cite this headnote

Appeals from the United States District Court for the Southern District of Texas, USDC No. 4:14–CV–237

Attorneys and Law Firms

Patrick W. Mizell, Deborah Carleton Milner, Vinson & Elkins, L.L.P., David H. Brown, Attorney, Brown & Kornegay, L.L.P., Houston, TX, for Plaintiff–Appellee Cross–Appellant.

Francis Joseph Nealon, Michael Albert Graziano, Attorney, Eckert, Seamans, Cherin & Mellott, L.L.C., Washington, DC, William Gaynor Winget, *253 Harris Bruce Katz, Garry T. Stevens, Jr., New York, NY, Martin Samuel Schexnayder, Esq., Houston, TX, Winget, Spadafora & Schwartzberg, L.L.P., for Defendant–Appellant Cross–Appellee.

Michael Keeley, Carla Cash Crapster, Strasburger & Price, L.L.P., Dallas, TX, for Amicus Curiae Surety & Fidelity Association of America.

Before JOLLY, BARKSDALE, and SOUTHWICK, Circuit Judges.

Opinion

PER CURIAM*

Texas law controls this diversity action, which arises out of Apache Corporation's being defrauded by criminals, in part by their use of an email; as a result of the fraud, and a flawed follow-up investigation by Apache, it made authorized payments of legitimate invoices from its vendor to the criminals' bank account, instead of to its vendor's. Great American Insurance Company (GAIC), Apache's insurer, denied its claim for coverage of its loss under GAIC's "Computer Fraud" provision of Apache's crime-protection insurance policy. At issue is whether the district court correctly awarded summary judgment to Apache, on the basis that its loss was covered under that provision; and, if so, whether the court properly denied statutory penalties, subject to Texas Insurance Code § 542.060. VACATED and RENDERED.

I.

GAIC is headquartered in Ohio; Apache is an oil-production company, with its principal place of business in Houston, Texas, but operating internationally. In March 2013, during the coverage period for Apache's policy with GAIC, an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed Apache to change the bank-account information for its payments to Petrofac. The Apache employee replied that the change-request could not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts-payable department received an email from a "petrofacld.com" address. But, Petrofac's authentic email domain name is "petrofac.com"; the criminals created "petrofacld.com" to send the fraudulent email. The email advised: Petrofac's "accounts details have now been changed"; and "[t]he new account takes ... immediate effect and all future payments must now be made into this account". As noted in the email, an attachment to it was a signed letter on Petrofac letterhead, providing both old-bank-account information and the new-bank-account number, with instructions to "use the new account with immediate effect". In addition, the email stated: the "attached letter ... has also been posted to you".

In response, an Apache employee called the telephone number provided on the letterhead to verify the request and concluded the call confirmed the authenticity of the change-request; next, a different Apache employee approved and implemented the change. A week later, Apache was transferring funds for payment of Petrofac's invoices to the new bank account.

Within one month, however, Apache received notification Petrofac had not received the £4.3 million (approximately \$7 million) Apache had transferred to the new (fraudulent) account. After an investigation *254 determined the criminals were likely based in Latvia, Apache recouped a substantial portion of the funds. It contends, however, it suffered a loss, before the \$1 million policy deductible, of approximately £1.5 million (approximately \$2.4 million).

Apache submitted a claim to GAIC, asserting coverage under the "Computer Fraud" provision, which states:

We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:

- a. to a person (other than a messenger) outside those premises; or
- b. to a place outside those premises.

In its denial letter, GAIC advised Apache's "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds".

Apache initiated this action in Texas state court in January 2014 against GAIC for denying its claim under the computer-fraud provision. After GAIC removed the action to district court, both parties moved for summary judgment.

The court denied GAIC's motion and granted Apache's, ruling, *inter alia*, "the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor' ". *Apache Corp. v. Great Am. Ins. Co.*, Civil Action No. 4:14-CV-237, 2015 WL 7709584, at *3 (S.D. Tex. 7 Aug. 2015). Moreover, the court reasoned that, if the policy only covered losses due to computer hacking, such an interpretation would render the policy "pointless". *Id.*

Apache moved for entry of final judgment, and sought, *inter alia*, statutory penalties under Texas Insurance Code

§ 542.060. But, in entering judgment, the court denied the penalties.

II.

GAIC challenges the summary judgment awarded Apache; on the other hand, Apache challenges the denial of statutory penalties. Because we vacate the judgment and render it for GAIC, we do not reach the penalties issue.

A summary judgment is reviewed *de novo*. *E.g.*, *Southern Ins. Co. v. Affiliated FM Ins. Co.*, 830 F.3d 337, 343 (5th Cir. 2016). Summary judgment is proper if the movant shows no genuine dispute as to any material fact and entitlement to judgment as a matter of law. Fed. R. Civ. P. 56(a). “The court must view the facts developed below in the light most favorable to the nonmoving party.” *La. Generating, L.L.C. v. Ill. Union Ins. Co.*, 831 F.3d 618, 622 (5th Cir. 2016). A genuine dispute of material fact exists “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party”. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). Interpretation of an insurance policy presents a question of law; therefore it is also reviewed *de novo*. *E.g.*, *Naquin v. Elevating Boats, L.L.C.*, 817 F.3d 235, 238 (5th Cir. 2016).

The summary-judgment record is very limited—there were no depositions or discovery responses. For its motion, GAIC attached: Apache’s proof of loss and supporting documents, such as the email at issue and the letterhead attachment to it; the crime-protection policy; and Apache’s declination letter. Apache relied on GAIC’s exhibits, in addition to two very brief, self-serving declarations executed by two Apache employees.

As noted, Texas law controls this diversity action. GAIC claims, *inter alia*, the loss was not a covered occurrence because: *255 the email did not “cause a transfer”; and coverage under this provision is “unambiguously limited” to losses from “hacking and other incidents of unauthorized computer use”. GAIC notes that, under Texas law, insurance provisions are interpreted according to the same rules applicable to contracts generally; but, it also asserts the “Supreme Court of Texas has ‘repeatedly stressed the importance of uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions’ ”, citing *McGinnes Indus. Maint. Corp. v. Phoenix Ins. Co.*, 477 S.W.3d 786, 794 (Tex.

2015). According to GAIC, the weight of authorities interpreting similar computer-fraud language, considered with Texas’ policy goal of cross-jurisdictional uniformity, persuades against coverage for Apache’s claim.

Apache counters that the plain meaning of the computer-fraud language covers its loss, and maintains any ambiguity in the terms should be resolved in favor of the insured’s reasonable interpretation, even if the insurer’s interpretation is more reasonable, relying on *RSUI Indem. Co. v. Lynd Co.*, 466 S.W.3d 113, 118 (Tex. 2015). Because the language of the provision says nothing about “hacking”, Apache asserts it only needs to show that “any computer was used to fraudulently cause the transfer of funds”.

As noted, under Texas law, courts interpret insurance policies using the same rules of construction applicable to contracts generally. *Tesoro Ref. & Mktg. Co., L.L.C. v. Nat’l Union Fire Ins. Co. of Pitt., Pa.*, 833 F.3d 470, 474 (5th Cir. 2016); *Am. Mfrs. Mut. Ins. Co. v. Schaefer*, 124 S.W.3d 154, 157 (Tex. 2003). The policy must be construed such that no provision is rendered meaningless. *Tesoro*, 833 F.3d at 474 (citing *Schaefer*, 124 S.W.3d at 157).

Mere disagreement about the meaning of a contract does not render it ambiguous. *Id.* “A contract is ambiguous only when the application of pertinent rules of interpretation to the face of the instrument leaves it genuinely uncertain which one of two or more meanings is the proper meaning.” *Id.* (quoting *RSUI Indem.*, 466 S.W.3d at 119). The ambiguity, *vel non*, of an insurance provision is a question of law; if ambiguity is found, the court must adopt the interpretation favoring the insured. *Id.* (citing *RSUI Indem.*, 466 S.W.3d at 118; *Schaefer*, 124 S.W.3d at 157).

As also noted, the Texas Supreme Court has stressed its policy preference for “uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions”. *McGinnes*, 477 S.W.3d at 794 (responding to fifth circuit certified question). And, even when uniformity is made impossible by jurisdictional splits, Texas courts “strive for uniformity as much as possible”. *Id.* (internal quotation marks omitted) (quoting *Trinity Universal Ins. Co. v. Cowan*, 945 S.W.2d 819, 824 (Tex. 1997)).

For our *Erie*-guess, the parties agree that only the computer-fraud provision is at issue. In contending Apache’s loss is not covered under it because the loss did not, as required by the provision, “result[] directly from the use of any computer to fraudulently cause a transfer”,

GAIC maintains the transfer of funds to the fraudulent bank account resulted from other events: before the email, the telephone call directing Apache to change the account information; and, after the email, the telephone call by Apache to the criminals to confirm the change-request, followed by the Apache supervisor's review and approval of the emailed request, Petrofac's submission of invoices, the review and approval of them by Apache employees, and Apache's authorized and intentional transfer of funds, even though to the fraudulent bank account. (As discussed, the email *256 stated that the attached letter on Petrofac letterhead "has also been posted [mailed] to" Apache. There is no evidence in the summary-judgment record, however, that Apache received a hardcopy of the letter. Nor is there any evidence Apache relied on one, as opposed to the electronic version attached to the fraudulent email, in telephoning to confirm the information provided. In any event, although this mailed-letter point was presented by GAIC at oral argument here, it is waived because it was not raised in district court or in GAIC's opening brief on appeal, with the alleged mailing of the letter only noted belatedly in its reply brief.)

In response to GAIC's position, Apache claims the loss is covered, based on the "commonly understood meaning" of the computer-fraud-provision's terms. It asserts GAIC attempts to add terms it wishes had been included in the provision.

The parties do not cite any Texas authority interpreting "the use of any computer to fraudulently cause a transfer" in the context of the computer-fraud provision, nor have we found any. Instead, GAIC relies primarily on unpublished opinions as persuasive authority; none are by Texas courts and almost all are outside our circuit. Apache attempts to distinguish them. Bearing in mind the limited weight accorded such non-binding authority, as well as Texas' policy preference for cross-jurisdictional uniformity, a detailed—albeit numbing—analysis of the cited authorities is required. See *McGinnes*, 477 S.W.3d at 794.

GAIC cites the ninth circuit's decision in *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, affirming coverage-denial under a similarly worded computer-fraud provision. (*Pestmaster II*), No. 14–56294, 656 Fed.Appx. 332, 333, 2016 WL 4056068, at *1 (9th Cir. 29 July 2016), *aff'g* *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.* (*Pestmaster I*), No. CV 13–5039–JFW, 2014 WL 3844627 (C.D. Cal. 17 July 2014) (unpublished). That policy defined "computer fraud" as "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property". *Pestmaster I*,

2014 WL 3844627, at *4.

The underlying fraud was committed by a payroll contractor against the insured. *Id.* at *1. The contractor had been hired, *inter alia*, to withhold and submit payments for the insured's payroll taxes. *Id.* To that end, the contractor prepared invoices for the insured, and was authorized to initiate transfers of funds from the insured to the contractor's bank account, in order to pay invoices approved by the insured. *Id.* (The district court considered the contractor's initiating the transfer of funds as the relevant "use of a computer". *Id.* at *7–8.) Instead of paying the approved invoices, the contractor fraudulently used the insured's funds to pay her own expenses, ultimately leaving the insured indebted to the Internal Revenue Service for payroll taxes. *Id.* at *2, 7–8.

The insured filed an action after being denied coverage under the crime-protection policy for the tax debt; but, the district court rejected coverage under the computer-fraud provision because the "claimed losses did not 'flow immediately' and 'directly' from [the contractor's] use of a computer". *Id.* at *8. "[T]here was no loss when funds were initially transferred to [the contractor] because the transfers were authorized by [the insured]". *Id.*

In affirming, the ninth circuit interpreted "the phrase 'fraudulently cause a transfer' to require an unauthorized transfer of funds". *Pestmaster II*, 2016 WL 4056068, at *1. "Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some *257 point in the transaction would convert this Crime Policy into a 'General Fraud' Policy", essentially covering losses from all forms of fraud rather than a specified risk category. *Id.*

GAIC also cites *Brightpoint, Inc. v. Zurich Am. Ins. Co.*, in which a district court ruled similar policy language did not cover a loss claimed by an insured distributor of prepaid mobile-telephone cards. No. 1:04–CV–2085–SEB–JPG, 2006 WL 693377, at *7 (S.D. Ind. 10 March 2006) (unpublished). After the distributor received a facsimile-transmission of purchase orders, postdated checks, and bank guarantees from a purported customer, the distributor delivered the inventory in exchange for the original documents. *Id.* at *2. The transaction was a fraud, with the distributor's never receiving payment. *Id.* at *3.

The court assumed, without deciding, that the facsimile-transmission constituted "use of a computer". In concluding the loss was not covered, it stated:

We do not view the faxed [documents] to have “fraudulently cause[d] a transfer” of the phone cards, as required under the policy definition of “Computer Fraud.” ... [T]he facsimile simply alerted the [insured] to the fact that [the insured’s customer], or perhaps in this case some other person mimicking his methods, wished to place an order. Only after [the insured] received the physical documents would [it] release the phone cards and, based on established practices of [the insured], the cards would not have been turned over simply on the basis of the facsimile.

Id. at *7.

Additionally, GAIC points to a summary-judgment ruling in its favor by the Northern District of Texas. *See GAIC v. AFS/IBEX Fin. Servs., Inc.*, No. 3:07–CV–924–O, 2008 WL 2795205, at *2 (N.D. Tex. 21 July 2008) (unpublished). There, an employee of the insured insurance-premium-finance company used a computer to submit more than 100 false loan applications to induce the insured to issue checks that the employee deposited for personal use. *Id.* The insured’s claim with GAIC sought coverage under, *inter alia*, the computer-fraud provision of a crime-protection insurance policy; the claim was denied. *Id.*

As in this instance, the computer-fraud provision covered a loss “resulting directly from the use of any computer to fraudulently cause a transfer of ... property”. *Id.* at *14. The court interpreted this language as being “designed to cover losses *directly* stemming from fraud perpetrated by use of a computer”. *Id.* (emphasis in original). Notably, the insured did not present “any evidence or arguments in opposition” to GAIC’s claiming the provision did not apply, but the court nonetheless determined the loss was not covered. *Id.*

As GAIC notes, similar policy language was at issue in *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, but the court denied the insurer’s motion to dismiss and allowed the insured’s claim to go forward. No. 11–6187, 2012 WL 1067694, at *4 (D. N.J. 29 March 2012) (unpublished). The facts considered in *Vonage*, however, differ from those here, because the insured was unquestionably “hacked”—hackers gained access to the insured’s servers

to fraudulently route international telephone calls. *Id.* at *1.

The only decision discussed by the parties which ruled the policy language covered computer-use limited to email communications was later vacated by the Superior Court of Connecticut. *See Owens, Schine, & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, 50 Conn. L. Rptr. 665, 2010 WL 4226958, at *8 (Conn. Super. Ct. 20 Sept. 2010) (unpublished), *258 vacated, 2012 WL 12246940 (Conn. Super. Ct. 18 Apr. 2012) (unpublished). The policy at issue defined “computer fraud” as “[t]he use of any computer to fraudulently cause a transfer”. *Id.* at *4.

The insured, a law firm, was defrauded by criminals who sent emails to the firm, representing themselves as Chinese businessmen in need of legal services. *Id.* at *1. All communications between the firm and the criminals were carried out by email. *Id.* at *7. A retainer agreement was signed, scanned, and emailed to the firm by the criminals. *Id.* at *1. They claimed they needed the firm’s services to collect a debt owed by an American company. *Id.* After a fraudulent check was received by the firm from the supposed debtor, the firm deposited the check in its trust account. *Id.* The firm then successfully wired funds from that account to one in South Korea; but, after the firm’s bank discovered the fraud, it refused to honor the fraudulent check provided by the criminals to the firm, resulting in its financial loss. *Id.* at *2.

In denying the insurer’s summary-judgment motion, the court ruled “[t]he emails were the proximate cause and ‘efficient cause’ of [the insured’s] loss because the [emails] set the chain of events in motion that led to the entire loss”. *Id.* at *8. As discussed, the decision, however, was vacated by the very court that rendered it.

Again, this vacated trial-court ruling is the only presented decision interpreting the computer-fraud policy language to cover a loss when the computer use at issue was limited to email correspondence. Therefore, with the exception of the district court’s ruling at issue, there is cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly by the computer use.

Here, the “computer use” was an email with instructions to change a vendor’s payment information and make “all future payments” to it; the email, with the letter on Petrofac letterhead as an attachment, followed the initial telephone call from the criminals and was sent in response to Apache’s directive to send the request on the vendor’s letterhead. Once the email was received, an Apache employee called the telephone number provided on the

fraudulent letterhead in the attachment to the email, instead of, for example, calling an independently-provided telephone contact for the vendor, such as the pre-existing contact information Apache would have used in past communications. Doubtless, had the confirmation call been properly directed, or had Apache performed a more thorough investigation, it would never have changed the vendor-payment account information. Moreover, Apache changed the account information, and the transfers of money to the fraudulent account were initiated by Apache to pay legitimate invoices.

The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in *Pestmaster II*, convert the computer-fraud provision to one for general fraud. See 2016 WL 4056068, at *1. We take judicial notice that, when the policy was issued in 2012, electronic communications were, as they are now, ubiquitous, and even the line between “computer” and “telephone” was already blurred. In short, few—if any—fraudulent schemes would not involve some form of computer-facilitated communication.

This is reflected in the evidence at hand. Arguably, Apache invited the computer-use at issue, through which it now seeks *259 shelter under its policy, even though the computer-use was but one step in Apache’s multi-step, but flawed, process that ended in its making required and authorized, very large invoice-payments, but to a fraudulent bank account.

The email was sent only after Apache’s advising, in reply to the criminals’ change-request telephone call, that the request had to be made on Petrofac letterhead. The criminals complied: by attaching to the email (sent using a slightly different domain name) a letter on altered letterhead; and, as stated in the email, by allegedly mailing that letter to Apache. Accordingly, the computer-use was in response to Apache’s refusing, during the telephone call, to, for example, transcribe the

change-request, which it could have then investigated with its records.

No doubt, the better, safer procedure was to require the change-request to be made on letterhead, especially for future payment of Petrofac’s very large invoices. But the request must still be investigated properly to verify it is legitimate. In any event, based on the evidence in the summary-judgment record, Apache followed-up on the request in the email and its attachment. In other words, the authorized transfer was made to the fraudulent account only because, after receiving the email, Apache failed to investigate accurately the new, but fraudulent, information provided to it.

Moreover, viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache elected to pay legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers.

In sum, and applying Texas law in making this *Erie* guess, both the plain meaning of the policy language, as well as the uniform interpretations across jurisdictions, dictate Apache’s loss was not a covered occurrence under the computer-fraud provision. See *McGinnes*, 477 S.W.3d at 794.

III.

For the foregoing reasons, the judgment is VACATED and judgment is RENDERED for Great American Insurance Company.

All Citations

662 Fed.Appx. 252

Footnotes

* Pursuant to 5th Cir. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5th Cir. R. 47.5.4.

End of Document

© 2019 Thomson Reuters. No claim to original U.S. Government Works.

2016 WL 6217161

Only the Westlaw citation is currently available.
United States District Court,
N.D. Alabama, Middle Division.

CAMP'S GROCERY, INC., Plaintiff,
v.
STATE FARM FIRE & CASUALTY COMPANY, Defendant.

Case No. 4:16-cv-0204-JEO

10/25/2016

JOHN E. OTT, Chief United States Magistrate Judge

MEMORANDUM OPINION

*1 The plaintiff in this action, Camp's Grocery, Inc. ("Camp's"), seeks a declaratory judgment that its insurer, defendant State Farm Fire & Casualty Company ("State Farm"), is obliged to defend and indemnify Camp's in connection with an underlying lawsuit brought against it in Alabama state court. (Doc' . 1). The parties have consented to an exercise of plenary jurisdiction by a United States Magistrate Judge pursuant to 28 U.S.C. § 636(c). (Doc. 8). The cause now comes to be heard on cross-motions for summary judgment. (Docs. 11, 12). Upon consideration, the court concludes that State Farm's motion for summary judgment is due to be granted and that Camp's cross-motion is due to be denied.

I. BACKGROUND

The objective material facts of this case are undisputed. Camp's operates a grocery store in Hokes Bluff, Alabama. It has been sued, along with its franchisor, Piggly Wiggly, LLC, and fictitiously identified defendants, in a lawsuit filed in the Circuit Court of Etowah County, Alabama. (Doc. 1-1). The plaintiffs in that underlying suit are three credit unions (the "Credit Unions"). They allege that Camp's computer network was hacked, compromising confidential **data** on its customers, including their credit card, debit card, and check card information. That **breach**, the Credit Unions claim, caused them to suffer losses on their cardholder accounts, including for reissuance of cards, reimbursement of their customers for fraud losses, lost interest and transaction fees, lost customers, diminished good will, and administrative expenses associated with investigating, correcting, and preventing fraud. The Credit Unions maintain that Camp's is liable for such damage on the theory that the **data breach** was caused by Camp's failure to provide adequate computer systems and employee training and/or to maintain adequate encryption and intrusion detection and prevention systems. Based on such allegations, the Credit Unions raise claims against Camp's under Alabama law claims for negligence, wantonness, misrepresentation, and **breach** of contract, as well as under federal law for violation of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* Camp's, in turn, has filed the instant action against State Farm, demanding a declaratory judgment under 28 U.S.C. § 2201(a) establishing that State Farm must defend and indemnify Camp's in the underlying action. This court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1332.²

*2 The State Farm policy under which Camp's seeks coverage (Doc. 11-3, the "Policy") contains two principal sections, which are respectively captioned, "Section I -- Property" and "Section II -- Liability." (Doc. 11-3 at 54-55). The general insuring clause of Section I contains a promise by State Farm to "pay for accidental direct physical loss to...Covered Property," encompassing "Buildings" ("Coverage A") and "Business Personal Property" ("Coverage B"), to the extent provided in the Declarations. (*Id.* at 56). "Business Personal Property" is defined to include "Property, used in your business,

that you own, lease from others or rent from others, or that is loaned to you," as well as "Property of others that is in your care, custody or control...." (*Id.*, Coverage B - Business Personal Property, ¶¶ 1, 2). However, "Covered Property" expressly does not include "electronic data." (*Id.* at 57, Property Not Covered ¶ 9; *see also id.* at 75, Section I - Definitions ¶ 5). Similarly, the term "Accident" is defined as not including "any defect, programming error, programming limitation, computer virus, malicious code, loss of 'electronic data', loss of access, loss of use, loss of functionality or other condition within or involving 'electronic data' of any kind." (*Id.* at 74, Section I - Definitions ¶ 1).

Turning to Section II of the Policy, the "Liability" insurance embodied therein includes a "Coverage L" for "Business Liability." (*Id.* at 76). The general insuring clause of that section states in relevant part:

[State Farm] will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury,' 'property damage,' or 'personal and advertising injury' to which this insurance applies. [State Farm] will have the right and duty to defend the insured by counsel of our choice against any "suit" seeking those damages. However, [State Farm] will have no duty to defend the insured against any "suit" seeking damages for "bodily injury," "property damage" or "personal and advertising injury", to which this insurance does not apply. We may, at our discretion, investigate any "occurrence" or offense and settle any claim or "suit" with or without the insured's consent, for any reason and at any time.

(*Id.* at 76, Coverage L ¶ 1). Section II also contains provisions specifically addressing computers and electronic data. First, the term "property damage" as used in Section II is limited to liability for harm to "tangible property," which is defined not to include "electronic data." (*Id.* at 89, Section II - Definitions ¶ 21). And expressly excluded from liability coverage under Section II are "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." (*Id.* at 81-82, Section II - Exclusions ¶ 18).

Camp's claim against State Farm, however, does not rely upon the provisions of either Section I or Section II of the Policy read in isolation. Instead, Camp's theory that State Farm owes it a defense and indemnity is based primarily upon two forms or endorsements attached to the Policy, one entitled, "FE-8743 Inland Marine Computer Property Form" (Doc. 11-3 at 43-46 ("IMCPF")), and the other, "FE-8739 Inland Marine Conditions." (*Id.* at 40-42 ("IMC")) (collectively the "Inland Marine endorsements"). Together, these contain terms and conditions of "Inland Marine" coverage. Indeed, the only provisions of the Policy that Camp's expressly references in, or attaches to, its complaint are the Inland Marine endorsements. (*See* Doc. 1 ¶¶ 16, 17; Doc. 1-2).

The IMCPF contains a general insuring provision stating in relevant part as follows:

INSURING AGREEMENT

We will pay for accidental direct physical loss to:

1. "Computer equipment", used in your business operations, that you own, lease from others, rent from others, or that is loaned to you....
2. Removable data storage media used in your business operations to store "electronic data".

* * *

We do not insure "computer programs" or "electronic data" except as provided in

the Computer Programs and Electronic Data Extension of Coverage. (Doc. 11-3 at 43). The extension of coverage referenced above, in turn, provides in relevant part:

EXTENSIONS OF COVERAGE

1. Computer Programs And Electronic Data

*3 a. We will pay for accidental direct loss to:

(1) The following types of "computer programs" and "electronic data" that you own, license from others, lease from others, or rent from others:

(a) "Computer programs" used in your business operations;

(b) The "electronic data" that exists in "computer" memory or on "computer" storage media, used in your business operations;

(2) That portion of your customers' "electronic data" that is supplied to you for processing or other use in your business operations. Coverage for customers' "electronic data" is limited to the specific data file(s) containing the information you are processing or using in your business operations.

We do not cover any property you lease to others, rent to others or license to others. We do not cover "computer equipment" or removable data storage media under this Extension Of Coverage. This coverage extension is included in the Limit Of Insurance shown on the Schedule Page.

Loss does not include any consequential loss except as may be provided in the optional Loss Of Income And Extra Expense coverage.

(Doc. 11-3 at 44). The above-referenced "optional Loss of Income and Extra Expense coverage" in the IMCPF provides in relevant part:

OPTIONAL COVERAGE - LOSS OF INCOME AND EXTRA EXPENSE

1. If a limit is shown on the Inland Marine Schedule Page for Loss Of Income And Extra Expense, coverage under this form is provided, subject to that limit, for the following:

a. The actual "Loss Of Income" you sustain due to the necessary "suspension" of your operations during the "period of restoration". The "suspension" must be caused by damage or destruction to property covered under this form, by a Covered Cause Of Loss;

b. Any necessary "extra expense" you incur during the "period of restoration" that you would not have incurred if there had been no damage or destruction to property covered under this form, by a Covered Cause Of Loss.

We will only pay for "Loss Of Income" or "extra expense" that you sustain during the "period of restoration" that occurs within 12 consecutive months after the date of loss. We will only pay for "ordinary payroll expenses" for 90 days following the date of loss.

2. We will not pay for:

a. Any "extra expense" or increase of "Loss Of Income" caused by suspension, lapse or cancellation of any license, lease or contract. But if the suspension, lapse or cancellation is directly caused by the "suspension" of your operations, we will cover such loss that affects your "Loss Of Income" during the "period of restoration";

b. Any "extra expense" caused by suspension, lapse or cancellation of any license, lease or contract beyond the "period of restoration";

c. Any other consequential loss;

d. Loss caused by seizure or destruction of property by order of governmental authority. But we will pay for acts of

destruction ordered by governmental authority and taken at the time of a fire to prevent its spread.

(Doc. 11-3 at 45).

The IMC then outlines certain conditions generally applicable to coverage and claims under IMCPF, including the following:

*4 Coverage in the Inland Marine Form is primary to any coverage provided in the policy this Form, is attached to, for the same property,

The following Conditions also apply:

1. **Agreement.** We agree to provide the insurance described in this policy. You agree to pay premiums when due and comply with the provisions of this policy.

* * *

4. **Loss Payment.** In the event of a loss covered by this policy:

* * *

b. We will not pay you more than your financial interest in the covered property.

c. We may adjust losses with the owners of lost or damaged property if other than you. If we pay the owners, such payments will satisfy your claims against us for the owners' property. We will not pay the owners more than their financial interest in the covered property;

d. We may elect to defend you, at our expense, against suits arising from claims of owners of property;

(Doc. 11-3 at 40).

The parties have now filed cross-motions for summary judgment on Camp's claim seeking a declaratory judgment, with each side relying upon the provisions of the Policy and the Credit Unions' complaint in the underlying suit. State Farm filed its motion first. (Doc. 11). Camp's cross-motion followed as part of Camp's response in opposition to State Farm's motion. (Doc. 12). The motions have been fully briefed¹ (see Doc. 11, 12, 13, 14) and are now ripe for decision.

II. REVIEW STANDARDS

Pursuant to Rule 56 of the FEDERAL RULES OF CIVIL PROCEDURE, a party is authorized to move for summary judgment on a claim or defense asserted by or against the movant. Under that rule, the "court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. PROC. 56(a). "Disposition of a summary judgment motion in a declaratory judgment action is governed by the same basic principles that generally rule the grant or denial of such a motion." *Bingham, Ltd. v. United States*, 724 F.2d 921, 924 (11th Cir. 1984).

The party moving for summary judgment "always bears the initial responsibility of informing the district court of the basis for its motion," relying on submissions "which it believes demonstrate the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986); see also *Clark v. Coats & Clark, Inc.*, 929 F.2d 604, 608 (11th Cir. 1991); *Adickes v. S.H. Kress & Co.*, 398 U.S. 144 (1970). Where the movant will not bear the burden of proof on a claim or issue at trial, the movant can satisfy that burden by pointing to specific portions of the materials on file that either negate an essential element of the non-movant's claim or that affirmatively indicate "that the party bearing the burden of proof at trial will not be able to meet that burden." *Clark*, 929 F.2d at 608; see also *Four Parcels*, 941 F.2d at 1438 & n.19. By contrast, when the moving party has the burden of proof at trial, it must support its motion with credible evidence that would entitle it to a directed verdict if not controverted at trial. *Four Parcels*, 941 F.2d at 1438. "In other words, the moving party must show that, on all the essential elements of its case on which it bears the burden of proof at trial, no reasonable jury could find for

the nonmoving party." *Id.*

*5 Once the moving party has met its initial burden, the nonmoving party must "go beyond the pleadings" and refer the court to evidence demonstrating that there is a genuine issue for trial. *Celotex Corp.*, 477 U.S. at 324. In its review of the evidence, a court must credit the evidence of the non-movant and draw all justifiable inferences in the non-movant's favor. *Stewart v. Booker T. Washington Ins.*, 232 F.3d 844, 848 (11th Cir. 2000). At summary judgment, "the judge's function is not himself to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986).

The fact that each party has filed a motion for summary judgment does not alter the Rule 56 standards applicable to each one. "Cross-motions for summary judgment will not, in themselves, warrant the court in granting summary judgment unless one of the parties is entitled to judgment as a matter of law on facts that are not genuinely disputed." *United States v. Oakley*, 744 F.2d 1553, 1555 (11th Cir. 1984) (citation omitted); see also *Busby v. JRHBW Realty, Inc. d/b/a RealtySouth*, 642 F. Supp. 2d 1283, 1289 (N.D. Ala. 2009) ("The fact that both parties simultaneously are arguing that there is no genuine issue of fact, however, does not establish that a trial is unnecessary thereby empowering the court to enter judgment as it sees fit," citing *Wright, Miller & Kane, Federal Practice and Procedure* § 2720, at 327-28 (3d ed. 1998)). "When both parties move for summary judgment, the court must evaluate each motion on its own merits, resolving all reasonable inferences against the party whose motion is under consideration." *Muzzy Products, Corp. v. Sullivan Indus., Inc.*, 194 F. Supp. 2d 1360, 1378 (N.D. Ga. 2002) (quoting *Gart v. Logitech, Inc.*, 254 F.3d 1334, 1338-39 (Fed. Cir. 2001)).

III. DISCUSSION

In support of its motion for summary judgment, State Farm argues that it has no duty to either defend or indemnify Camp's in the underlying action. First, State Farm asserts that, to the extent Camp's relies upon the IMCPF, that document cannot be read to provide for a defense or indemnity for legal claims brought against the insured by a third party for damage stemming from lost or compromised electronic data. That is so because the IMCPF, State Farm contends, is a "first-party insuring agreement," meaning that it covers losses sustained directly by the insured itself. As such, State Farm insists, the IMCPF is not a "third-party insuring agreement" that may afford a defense and indemnity where the insured is sued to redress a loss suffered by another party, which is what Camp's has demanded. On the other hand, State Farm acknowledges that Coverage L for "Business Liability" in Section II of the Policy does contain a third-party insuring agreement. State Farm maintains, however, that for Coverage L to apply, the third party's claim for damages must be based on allegations that the insured's misconduct caused the third party to suffer "bodily injury," "property damage," or "personal and advertising injury," as those terms are defined in the Policy. And the Credit Unions' claims in underlying suit, State Farm says, do not qualify. For the reasons explained below, the court agrees with State Farm.

The Alabama Supreme Court⁴ has recognized as follows with regard to the distinction between first-party insurance coverage and third-party coverage, as follows:

"Insurance contracts generally are assigned to one of two classes: either 'first-party coverage' or 'third-party coverage'....'First-party coverage' pertains to loss or damage sustained by an insured to its property; the insured receives the proceeds when the damage occurs....In contrast, if the insurer's duty to defend and pay runs to a third-party claimant who is paid according to a judgment or settlement against the insured, then the insurance is classified as 'third-party insurance'....Thus, wholly different interests are protected by first-party coverage and third-party coverage.

*6 "...The interests protected...involve property, not persons. Indeed, the goal of first-party property coverage, including fire, builder's risk and installation risk, is to reimburse the insured for the insured's actual property loss, dollar for dollar, but no more.

Colony Ins. Co. v. Georgia-Pac., LLC, 27 So. 3d 1210, 1214-15 (Ala. 2009) (quoting *Great Northern Ins. Co. v. Mount Vernon Fire Ins. Co.*, 708 N.E.2d 167, 170-71 (N.Y. 1999)); see also *Aetna Cas. & Sur. Ins. Co. v. State ex rel. Eagerton*, 414 So. 2d 455, 457 (Ala. 1982) ("[F]irst party claims are those by a policyholder for damage to his property. Third party claims are those of a person contending that a policyholder is liable to him for damage to him."); *Toffel v. Nationwide Mut. Ins. Co.*, No. 2:15-cv-01669-KOB, 2016 WL 4271837, at *7 n. 3 (N.D. Ala. Aug. 15, 2016) (" 'First-party' insurance claims involve personal or property insurance," while " '[t]hird-party...claims involve liability insurance'").

To establish that State Farm owes a defense and indemnity, Camp's relies primarily upon the Inland Marine endorsements. (See Doc. 1 ¶¶ 16, 17; Doc. 1-2). However, there is no language in either the IMCPF or the IMC whereby State Farm promises to "defend" or "indemnify" the insured, whether in regard to claims involving computer equipment, electronic **data**, or anything else, for that matter. Rather, the general insuring agreement of the IMCPF provides: "[W]e will pay for accidental *direct physical loss* to...1. Computer equipment [and] 2. Removable **data** storage media." (Doc. 11-3 at 43 (emphasis added)). Similarly, the "Extensions of Coverage" in the IMCPF states: "We will pay for accidental *direct loss* to...(1)....(a) 'Computer programs used in your business operations; (b) The 'electronic **data**' that exists in 'computer' memory or on 'computer' storage media, used in your business operations; (2) That portion of your customer' 'electronic **data**' that is supplied to you for processing or other use in your business operations." (*Id.* at 44 (emphasis added)). Such promises to pay the insured's "direct loss" unambiguously afford first-party coverage only and do not impose a duty to defend or indemnify the insured against legal claims for harm allegedly suffered by others, as in third-party coverage. See *RVST Holdings, LLC v. Main St. Am. Assur. Co.*, 136 A.D.3d 1196, 1198, 25 N.Y.S.3d 712, 714 (N.Y. App. Div. 2016); *Butler v. Clarendon Am. Ins. Co.*, 494 F. Supp. 2d 1112, 1129 (N.D. Cal. 2007), *aff'd*, 317 F. App'x 648 (9th Cir. 2009); *Power Eng'g Co. v. Royal Ins. Co. of Amer.*, 105 F. Supp. 2d 1196, 1207 (D. Colo. 2000); *Shell Oil Co. v. Winterthur Swiss Ins. Co.*, 12 Cal. App. 4th 715, 765, 15 Cal. Rptr. 2d 815, 848 (1993), *reh'g denied and opinion modified* (Feb. 22, 1993); *Edward J. Gerrits, Inc. v. National Union Fire Ins. Co. of Pittsburgh, Penn.*, 634 So. 2d 712, 713 (Fla. Dist. Ct. App. 1994). Therefore, the terms of the IMCPF itself impose no obligation on State Farm to either defend or indemnify Camp's in the underlying action.

*7 Camp's highlights, however, that the IMC provides that, in the event of a covered loss, "[State Farm] may elect to defend [the insured], at [State Farm's] expense, against suits arising from claims of owners of property." (Doc. 11-3 at 40, ¶ 4(d)). Camp's reads such language to mean that State Farm has assumed a duty to defend the insured. The court disagrees. On its face, a policy provision that the insurer "may elect to defend" an insured unambiguously gives the insurer a discretionary choice or right to defend; it does not create a *duty*, that is a *nondiscretionary legal obligation*, to do so. See *Omega Demolition Corp. v. Travelers Prop. Cas. of Am.*, No. 14-CV-01288, 2015 WL 3857341, at *4 (N.D. Ill. June 19, 2015); *Genaeys Corp. v. Harco Nat'l Ins. Co.*, 991 A.2d 342, 349 (Pa. Super. Ct. 2010); *Stadium Lincoln-Mercury, Inc. v. Heritage Transport*, 826 N.E.2d 332, 337 (Ohio Ct. App. 2005); *Nourishad v. SCPIE Indem. Co.*, No. G035218, 2006 WL 1015756, at *11 (Cal. Ct. App. Apr. 19, 2006); see also Stephen E. Goldman & John W. Steinmetz, Property Insurers' Rights and Obligations Under Policy Provisions That Provide Coverage for Personal Property of Others, 32 Tort & Ins. L.J. 787, 798 (1997) ("[T]he ISO Businessowners Standard Property Coverage Form provides that the insurer 'may elect to defend [its insured] against suits arising from claims of owners of property.' Under the law of most states, this language does not create an obligation to defend; it merely gives the insurer the right to defend actions filed against its insureds.").

Camp's replies that the IMC language providing that State Farm "may elect to defend" is nonetheless ambiguous in light of other provisions of the Policy. (See Doc. 12 at 11-13). More specifically, Camp's seems to claim that, even if the Inland Marine endorsements themselves do not create or acknowledge a duty to defend, it is undisputed that Coverage L in Section II of the Policy provides liability insurance under which State Farm has assumed a duty to defend and indemnify. According to Camp's, the Inland Marine endorsements expand the scope of liability insurance under Coverage L such that State Farm must render a defense and indemnity for claims based on losses involving computers and electronic **data**. Again, the court disagrees.

It is true that Coverage L supplies business liability **insurance** by which State Farm has assumed a duty to defend and indemnify Camp's against certain enumerated legal claims. However, as State Farm argues, Coverage L does not apply to any of the claims in the underlying suit. Coverage L's is triggered where the insured becomes legally obligated to pay damages because of "bodily injury," "property damage," or "personal and advertising injury." (Doc. 11-3 at 76, Coverage L - Business Liability ¶ 1). The underlying suit is brought by incorporated entities who claim purely economic loss as a result of alleged **cyber** attacks on Camp's computer network that compromised the security of electronic **data**, specifically, the debit and credit card information of their shared customers. Although State Farm clearly raises arguments that the underlying action does not involve either "bodily injury" or "personal and advertising injury" (Doc. 11 at 16, 20-22), Camp's does not respond to those arguments in its summary judgment brief. Accordingly, Camp's has abandoned those theories as a basis of recovery. See *Iraola & CIA, S.A. v. Kimberly-Clark Corp.*, 325 F.3d 1274, 1284-85 (11th Cir. 2003); *Resolution Trust Corp. v. Dunmar Corp.*, 43 F.3d 587, 599 (11th Cir. 1995); *Road Sprinkler Fitters Local Union No. 669 v. Independent Sprinkler Corp.*, 10 F.3d 1563, 1568 (11th Cir. 1994).

Camp's does argue, however, that the underlying suit seeks damages for "property damage," insofar as the Credit Unions allege that they suffered "losses for replacement customer debit and credit cards." (Doc. 12 at 9 (internal quotation marks omitted); *see also* Doc. 1-1 at 6, ¶ 8 ("Plaintiffs have incurred significant losses associated with credit and debit card reissuance"); *id.* at 11, ¶ 36 ("Plaintiffs had to protect their customers and avoid fraud losses; Cards they had issued, and reissue Cards with new account numbers and magnetic stripe information to customers."); *id.* ¶ 37 ("The cancellation and reissuance of cards resulted in damages and losses to Plaintiffs."). Camp's acknowledges that, for purposes of Coverage L, "property damage" is limited to "tangible property" and that "electronic data is not tangible property." (See Doc. 11-3 at 89, ¶ 21). Camp's suggests, however, that, since "the physical debit cards are not only 'electronic data,' but are [also] tangible property that can be touched and handled," (Doc. 12 at 9), the Credit Unions' claimed losses connected with replacing the cards is covered "property damage."

*8 But even if credit and debit cards are tangible property, Camp's argument is fatally flawed. The Credit Unions do not assert that Camp's acts or omissions caused physical harm or damage to any cards as tangible property. Rather, the Credit Unions assert that Camp's lax computer network security allowed the *intangible electronic data contained on the cards* to be compromised such that the magnetically encoded card numbers could no longer be used, causing purely economic loss flowing from the need to issue replacement cards with new electronic data. Moreover, Coverage L is subject to an exclusion for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." (*Id.* at 81-82, Section II - Exclusions ¶ 18). As a result, the Credit Unions' claims for damages arising out of Camp's allegedly unlawful handling of electronic data on the credit cards are not claims for "property damage" under the Policy and are excluded from coverage. *See RVST Holdings*, 136 A.D.3d at 1198, 25 N.Y.S.3d at 714; *see also American States Ins. Co. v. Martin*, 662 So. 2d 245, 249 (Ala. 1995) (insureds' purely economic loss was not covered as "property damage" under liability policy); Carole Basri, Mary Mack, *eDiscovery for Corporate Counsel* § 17:7 ("[C]ase law reveals that organizations may have a difficult time obtaining coverage under a CGL policy for claims arising from a cyber-breach.").

Nor do the provisions of Coverage L render the Inland Marine Endorsements ambiguous as it relates to a duty to defend. In essence, Camp's argues that, even if neither Coverage L nor the Inland Marine endorsements by their own terms apply to the Credit Unions' claims in the underlying action, if one takes the duty to defend from the third-party coverage of former and the first-party coverage for electronic data loss from the latter, read together they form an amalgamation providing liability insurance against claims for electronic data loss. That, however, is simply not what the Policy provides. Camp's suggests that it is merely interpreting the different coverages of the Policy as an integrated whole. But what Camp's is actually doing is selectively reading the Policy in a piecemeal fashion, picking and choosing parts of different coverages while conveniently ignoring other terms from those same coverages that would preclude or exclude their application to the Credit Unions' claims. Moreover, it is clear that, contrary to Camp's assertion, the provisions of the Inland Marine endorsements stand distinctly separate and apart from the business liability insurance afforded by Coverage L and do not expand it. Rather,

the [Inland Marine] Endorsement[s] act[] as a sort of "mini-policy." Like the Policy itself, the Endorsement[s] set[] forth an insuring agreement complete with its own definitions, detailed conditions, and deductible. The Endorsement[s] even ha[ve] something to say about exclusions. As we have seen, [they] specif[y] that certain existing exclusions do not apply to the Endorsement[s'] coverage, it modifies other exclusions, and it adds still others that are only applicable to the Endorsement[s].

AJC Int'l, Inc. v. Triple-S Propiedad, 790 F.3d 1, 9 (1st Cir. 2015). In the end, the Inland Marine endorsements afford only first-party coverage for certain computer equipment and electronic data, as specified in the IMCPF. Those endorsements do not create, recognize, or assume the existence of a duty to defend or indemnify against claims brought by third parties. As such, the Inland Marine endorsements are properly read as expanding or otherwise modifying not the third-party liability insurance of Coverage L in Section II of the Policy but rather the first-party property insurance of Section I, which, like the IMCPF, contains promises by State Farm to pay the insured's "direct loss" to enumerated property. (See Doc. 11-3 at 56 ("[W]e will pay for accidental direct physical loss to...Covered Property")). The court concludes that the language of the Policy is unambiguous and does not impose a duty on State Farm to defend or indemnify Camp's in the underlying action.⁶

IV. CONCLUSION

*9 Based on the foregoing, State Farm's motion for summary judgment (doc. 11) is due to be **GRANTED**, while Camp's cross-motion for summary judgment (doc. 12) is due to be **DENIED**. A separate final order will be entered.

DONE, this 25th day of October, 2016.

JOHN E. OTT

Chief United States Magistrate Judge

All Citations

Slip Copy, 2016 WL 6217161

Footnotes

- ¹ References to "Doc(s). ____" are to the document numbers assigned to the pleadings, motions, and other materials in the court file as compiled and designated by the Clerk of the Court. Unless otherwise noted, pinpoint citations are to the page of the electronically filed document in the court's CM/ECF system, which may not correspond to pagination on the original "hard copy" of the document presented for filing.
- ² An action for declaratory relief under the Declaratory Judgment Act, 28 U.S.C. § 2201(a), must independently satisfy subject matter jurisdiction requirements. *Vaden v. Discover Bank*, 556 U.S. 49, 70 n. 19 (2009). The district courts have original jurisdiction over civil actions between citizens of different states where the amount in controversy exceeds \$75,000. 28 U.S.C. § 1332(a)(1). For purposes of the diversity statute, Camp's is an Alabama citizen, while State Farm is an Illinois citizen. *See* 28 U.S.C. § 1332(c)(1); (Doc. 1 ¶¶ 3, 4, 5; Doc. 4 ¶¶ 3, 4, 5; Doc. 11-3 at 2 ("State Farm Fire and Casualty Company, A Stock Company with Home Offices in Bloomington, Illinois"); *State Farm Fire & Cas. Co. v. Rollins*, 2016 WL 2760351, at *2 (E.D. Va. May 12, 2016). Camp's has also claimed that the relief it seeks has value in excess of the jurisdictional minimum. (Doc. 1 ¶ 5).
- ³ Both parties have requested oral argument on their respective motions for summary judgment. (Doc. 11 at 1; Doc. 12 at 1). However, the court is not required to grant an oral hearing under Rule 56. *Moore v. State of Fla.*, 703 F.2d 516, 519 (11th Cir. 1983). And because the facts are undisputed and the court finds that the issues raised by the parties are adequately addressed by the briefs, oral argument would not be of significant aid and is therefore unnecessary. *See George W. Bennett Bryson & Co. v. Norton Lilly & Co.*, 502 F.2d 1045, 1051 (5th Cir. 1974).
- ⁴ Sitting in diversity, this court is bound to apply Alabama substantive law, while applying federal procedural law. *See Erie R. Co. v. Tompkins*, 304 U.S. 64 (1938); *Palm Beach Golf Center- Boca, Inc. v. John G. Sarris*, DDS, PA, 781 F.3d 1245, 1259-60 (11th Cir. 2015).
- ⁵ Even absent abandonment, the court would find that the underlying action does not allege "bodily injury" or "personal or advertising injury" for the reasons stated in State Farm's brief. (*See* Doc. 11 at 16, 20-22).
- ⁶ Plaintiff cites *American Safety Indemn. Co. v. National Union Fire Ins. Co. of Pittsburgh*, 759 F. Supp. 2d 1218 (S.D. Cal. 2011), and *Flowers v. Max Specialty Ins. Co.*, 761 S.E.2d 787 (W. Va. 2014), to support that the Policy is at least ambiguous as to State Farm's duty to defend. (Doc. 12 at 11-13). Both cases, however, are distinguishable. In *American Safety*, the district court held that language in an endorsement that the insurer had "the right but not the duty to defend" the insured was "plain" and did not itself impose an obligation to defend. 759 F. Supp. 2d at 1221-22. Despite that, the court found that the policy, read as a whole, was ambiguous because a different policy endorsement that also potentially applied to the claims at issue contained language that, on its face, "assume[d] the existence of a duty to defend." *Id.* at 1222. And under state law, that ambiguity had to be read against the insurer that issued the policy. *Id.* at 1222-23. But as discussed in the text, the Inland Marine endorsements here neither create nor acknowledge a duty to defend. More importantly, unlike in *American Safety*, the "other" portion of the Policy that purportedly engenders ambiguity, Coverage L, cannot be reasonably interpreted to apply to the claims in the underlying action, nor can the first-party **insurance** of the Inland Marine endorsements be read to expand or modify the third-party liability **insurance** of Coverage L.

Flowers also does not aid Camp's cause. There the issue was whether a general commercial liability (GCL) policy permitted the insurer to terminate its duty to defend at such time as the policy limit of \$25,000 is exhausted through the expenditure of

attorney's fees and costs. *See* 761 S.E.2d at 792. Ultimately, the court determined that the provisions in the "GCL coverage and [a] supplementary payments parts of the policy... regarding the duty to defend" were "contradictory to [an] endorsement" and that such "contradictory and confusing provisions creat[ed] significant ambiguity in the entire policy." *Id.* at 796. Construing such ambiguity in favor of the insured, the court held that the policy did not allow the insurer to terminate its duty to defend through expenditure of policy limits on attorney's fees and costs. *Id.* But again, in the case *sub judice*, there simply are not "contradictory" provisions as it might relate to State Farm's duty to defend the claims in the underlying action. To the contrary it is clear that State Farm has no duty to defend either under the Inland Marine endorsements, which afford only first-party coverage, or under the business liability provisions of Coverage L, which do not reach or otherwise exclude coverage for the Credit Unions' claims based on allegedly deficient ~~cyber~~ security.

End of Document

© 2016 Thomson Reuters. No claim to original U.S. Government Works.

2018 WL 6072199

Only the Westlaw citation is currently available.

Supreme Court of Pennsylvania.

Barbara A. **DITTMAN**, Gary R. Douglas, Alice
Pastirik, Joann Decolati, Tina Sorrentino, Kristen
Cushman and Shannon Molyneaux, Individually
and on Behalf of All Others Similarly Situated,
Appellants

v.

UPMC d/b/a The University of Pittsburgh Medical
Center, and UPMC McKeesport, Appellees

No. 43 WAP 2017

Argued April 10, 2018

Decided November 21, 2018

Synopsis

Background: Employees of university medical center brought class action against medical center for negligence and breach of implied contract after a data breach, wherein the names, birth dates, social security numbers, tax information, addresses, salaries, and bank information of employees were accessed and stolen from medical center's computer systems. The Court of Common Pleas, Allegheny County, Civil Division at No. GD14-003285, Stanton R. Wettick, Jr., J., sustained medical center's preliminary objections. Employees appealed. The Superior Court, No. 971 WDA 2015, 154 A.3d 318, affirmed. Employees sought allowance of appeal.

Holdings: The Supreme Court, No. 43 WAP 2017, Baer, J., held that:

[1] employer owed employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm in collecting and storing employees' data on its computer systems, and

[2] economic loss doctrine did not bar employees' negligence claim.

Judgment of the Superior Court vacated; order of the Court of Common Pleas reversed; remanded.

Saylor, C.J., filed concurring and dissenting opinion in which Todd, J., joined.

West Headnotes (11)

[1] Appeal and Error



The standard of review of pure questions of law is de novo.

Cases that cite this headnote

[2] Appeal and Error



The scope of review of pure questions of law is plenary.

Cases that cite this headnote

[3] Appeal and Error



When a claim has been dismissed on preliminary objections in the nature of a demurrer, the appellate court must determine whether, on the facts averred, the law says with certainty that no recovery is possible.

Cases that cite this headnote

[4] Appeal and Error



Any existing doubt as to whether a demurrer should be sustained should be resolved in favor of overruling it.

Cases that cite this headnote

risk of harm arising from employer's collection and storage of **employees' data** on its computer systems.

[5] **Appeal and Error**



In reviewing a demurrer, the appellate court accepts as true all material facts as set forth in the complaint and any inferences reasonably deducible therefrom in conducting its review.

Cases that cite this headnote

Cases that cite this headnote

[6] **Labor and Employment**



In collecting and storing **employees' data** on its computer systems, employer owed **employees** a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act; **employees** alleged that, as a condition of employment, employer required them to provide certain personal and financial information.

Cases that cite this headnote

[9] **Negligence**



The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although the actor's negligent conduct created a situation which afforded an opportunity to the third person to commit such a tort or crime, unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime.

Cases that cite this headnote

[7] **Negligence**



Generally, there is no duty to protect or rescue someone who is at risk on account of circumstances the defendant had no role in creating.

Cases that cite this headnote

[10] **Negligence**



The economic loss doctrine does not preclude all negligence claims seeking solely economic damages.

Cases that cite this headnote

[8] **Negligence**



Presence of third-party criminality did not eliminate employer's duty to exercise reasonable care to protect **employees** against unreasonable

[11] **Labor and Employment**



Economic loss doctrine did not bar **employees'** negligence claim against employer in which **employees** alleged that employer breached its common law duty to act with reasonable care in collecting and storing **employees'** personal and financial information on its computer systems; legal duty existed independently of any contractual obligations between parties.

Cases that cite this headnote

Appeal from the Order of the Superior Court entered January 12, 2017 at No. 971 WDA 2015, affirming the Order of the Court of Common Pleas of Allegheny County entered May 28, 2015 at No. GD14-003285.

SAYLOR, C.J., BAER, TODD, DONOHUE, DOUGHERTY, WECHT, MUNDY, JJ.

OPINION

JUSTICE BAER

*1 We granted discretionary review in this matter to determine whether an employer has a legal duty to use reasonable care to safeguard its **employees'** sensitive personal information that the employer stores on an internet-accessible computer system. We also examine the scope of Pennsylvania's economic loss doctrine, specifically whether it permits recovery in negligence for purely pecuniary damages. For the reasons discussed below, we hold that an employer has a legal duty to exercise reasonable care to safeguard its **employees'** sensitive personal information stored by the employer on an internet-accessible computer system. We further hold that, under Pennsylvania's economic loss doctrine, recovery for purely pecuniary damages is permissible under a negligence theory provided that the plaintiff can establish the defendant's breach of a legal duty arising under common law that is independent of any duty assumed pursuant to contract. As the Superior Court came to the opposite conclusions, we now vacate its judgment.

Barbara A. Dittman, Gary R. Douglas, Alice Pastirik, Joann Decolati, Tina Sorrentino, Kristen Cushman, and Shannon Molyneaux, individually and on behalf of all others similarly situated (collectively, **Employees**), filed the operative class action complaint in this matter against UPMC d/b/a the University of Pittsburgh Medical Center and UPMC McKeesport (collectively, UPMC) on June 25, 2014. In the complaint, **Employees** alleged that a data breach had occurred through which the personal and

financial information, including names, birth dates, social security numbers, addresses, tax forms, and bank account information of all 62,000 UPMC **employees** and former **employees** was accessed and stolen from UPMC's computer systems. Second Amended Class Action Complaint, 6/25/2014, at ¶¶ 21-22, 27, 53. **Employees** further alleged that the stolen data, which consisted of information UPMC required **Employees** to provide as a condition of their employment, was used to file fraudulent tax returns on behalf of the victimized **Employees**, resulting in actual damages. *Id.* ¶¶ 21, 23, 35.

Based on the foregoing, **Employees** asserted a negligence claim and breach of implied contract claim against UPMC.¹ With respect to their negligence claim, **Employees** alleged that UPMC had a duty to exercise reasonable care to protect their "personal and financial information within its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties." *Id.* at ¶ 53. **Employees** further alleged that UPMC undertook a duty of care to ensure the security of their information in light of the special relationship between **Employees** and UPMC, whereby UPMC required **Employees** to provide the information as a condition of their employment. *Id.* at ¶ 56. **Employees** averred that this "duty included, among other things, designing, maintaining, and testing its security systems to ensure" that **Employees'** information was adequately protected, and implementing "processes that would detect a breach of its security systems in a timely manner." *Id.* at ¶¶ 54-55.

*2 Additionally, **Employees** claimed that UPMC breached its duty to use reasonable care "by failing to adopt, implement, and maintain adequate security measures to safeguard [**Employees'**] ... information, failing to adequately monitor the security of its network, allowing unauthorized access to [**Employees'**] ... information, and failing to recognize in a timely manner that [**Employees'**] ... information had been compromised." *Id.* at ¶ 57. **Employees** further averred that UPMC "violated administrative guidelines" and "failed to meet current data security industry standards," specifically by failing to encrypt data properly, "establish adequate firewalls to handle a server intrusion contingency," and "implement adequate authentication protocol to protect the confidential information contained in its computer network." *Id.* at ¶¶ 33-34.

Employees also claimed that UPMC's breach of its duties was the direct and proximate cause of the harm to **Employees**. *Id.* at ¶¶ 59-60. Finally, **Employees** alleged that, as a result of UPMC's negligence, **Employees** "incurred damages relating to fraudulently filed tax

returns” and are “at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.” *Id.* at ¶¶ 61-62. Based on the foregoing, **Employees** sought monetary damages, among other forms of relief. *Id.* at ¶ 70.

On July 16, 2014, UPMC filed preliminary objections to **Employees’** complaint arguing that, *inter alia*, their negligence claim failed as a matter of law. Specifically, UPMC argued that no cause of action exists for negligence because **Employees** did not allege any physical injury or property damage and, under the economic loss doctrine, “no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage.” UPMC’s Preliminary Objections to **Employees’** Second Amended Class Action Complaint, 7/16/2014, at ¶¶ 15-17 (quoting *Excavation Technologies, Inc. v. Columbia Gas Co. of Pa.*, 604 Pa. 50, 985 A.2d 840, 841 n.3 (2009)). **Employees** responded in opposition, and UPMC filed a reply to **Employees’** response. Thereafter, on October 22, 2014, the parties appeared before the trial court for oral argument on UPMC’s preliminary objections. Following argument, at the court’s direction, both parties filed supplemental briefs addressing whether UPMC owed a duty of care to **Employees** under the five-factor test set forth in *Althaus ex rel. Althaus v. Cohen*, 562 Pa. 547, 756 A.2d 1166 (2000).²

On May 28, 2015, the court sustained UPMC’s preliminary objections and dismissed **Employees’** negligence claim.³ Relying upon the general description of the economic loss doctrine quoted from *Excavation Technologies* above, the trial court observed that, while **Employees** claimed that UPMC owed them a duty of care, the only losses **Employees** sustained were economic in nature. Trial Ct. Op., 5/28/2015, at 4. The trial court then briefly examined this Court’s decision in *Bilt-Rite Contractors, Inc. v. The Architectural Studio*, 581 Pa. 454, 866 A.2d 270 (2005), which allowed a negligence action based upon economic loss alone, viewing it as merely creating an exception to the economic loss doctrine for losses incurred as a result of a plaintiff’s reliance on advice given by professionals for pecuniary gain.⁴ *Id.* at 4-5. The trial court concluded that, because this “case does not involve defendants in the business of supplying information for economic gain,” the exception did not apply. *Id.*

^{*3} The trial court further opined that the *Althaus* factors and duty of care “should not be considered where the plaintiff seeks to recover only economic losses,” as “the Pennsylvania appellate courts have already balanced the competing interests through adoption of the economic

loss doctrine.” *Id.* at 5. This determination notwithstanding, the trial court went on to analyze the *Althaus* factors and conclude that courts should not impose “a new affirmative duty of care that would allow data breach actions to recover damages recognized in common law negligence actions.” *Id.* The trial court found the controlling factors of the *Althaus* test to be (1) the consequences of imposing a duty upon the actor, and (2) the overall public interest in the proposed solution. In this regard, the trial court observed that data breaches are widespread and frequent. The trial court further explained that, under **Employees’** proposed solution of creating a private negligence cause of action to recover actual damages resulting from data breaches, “hundreds of thousands of lawsuits” could result, which would overwhelm the judicial system and require entities to expend substantial resources in defending against those actions. *Id.* at 6. Additionally, the trial court reasoned that there are no generally accepted reasonable care standards for evaluating one’s conduct in protecting data, and that use of expert testimony and jury findings is not a viable method to develop those standards in data breach litigation. *Id.*

The trial court opined that it could not say with reasonable certainty that the best interests of society would be served through the recognition of a new affirmative duty under these circumstances, noting that the financial impact of doing so could put entities out of business. *Id.* at 7. The trial court further explained that entities storing confidential information already have an incentive to protect that information because any breach will affect their operations, that an improved system would not necessarily prevent a breach, and that the entities were also victims of the criminal activity involved. *Id.* at 7-8. Finally, the trial court observed that the Legislature is aware of and has considered the issues that **Employees** sought the court to consider herein as evidenced by the Breach of Personal Information Notification Act (*Data Breach Act*), 73 P.S. §§ 2301-2329. Specifically, the court explained that, under the *Data Breach Act*, the Legislature has imposed a duty on entities to provide notice of a data breach only, 73 P.S. § 2303, and given the Office of Attorney General the exclusive authority to bring an action for violation of the notification requirement, *id.* at § 2308. Trial Ct. Op., 5/28/2015, at 8-10. The court thus reasoned that, as public policy was a matter for the Legislature, it was not for the courts to alter the Legislature’s direction.⁵ *Id.* at 10.

Employees appealed to the Superior Court. Relevant to the issues before this Court, **Employees** argued that the trial court erred in finding that UPMC did not owe a duty of reasonable care in its collection and storage of

Employees' information, and that the economic loss doctrine barred their claim.

In a split opinion, a three-judge panel of the Superior Court affirmed the order of the trial court sustaining UPMC's preliminary objections and dismissing **Employees'** claims. *Dittman v. UPMC*, 154 A.3d 318 (Pa. Super. 2017). As to the issue of duty, the Superior Court applied the *Althaus* factors, concluding first that the relationship between the parties weighed in favor of imposing a duty on UPMC because the employer-employee relationship "traditionally has given rise to duties on the employer." *Id.* at 323. The court also reasoned that "[t]here is an obvious social utility" in electronically storing **employees'** personal information "to promote efficiency," which outweighed the nature of the risk imposed and foreseeability of the harm incurred in so doing. *Id.* at 323-24. While the court noted that the general risk of storing information electronically increases as **data** breaches become more common and that **data** breaches and the ensuing harm were generally foreseeable, "more and more information is stored electronically" in the modern era and "**employees** and consumers alike derive substantial benefits from" the resulting efficiencies. *Id.* at 323. The court further observed that "a third party committing a crime is a superseding cause" against which "a defendant does not have a duty to guard ... unless he realized, or should have realized, the likelihood of such a situation." *Id.*

*4 The Superior Court further agreed with the trial court's analysis of the fourth and fifth *Althaus* factors, the consequences of imposing a duty upon the actor and the overall public interest in the proposed solution, respectively. As to the fourth factor, the Superior Court added to the trial court's reasoning that no judicially created duty of care is needed to incentivize companies to protect their **employees'** confidential information because there are "statutes and safeguards in place to prevent employers from disclosing confidential information." *Id.* at 324 (citing, *inter alia*, the Data Breach Act). The Superior Court also found it "unnecessary to require employers to incur potentially significant costs to increase security measures when there was no true way to prevent **data** breaches altogether." *Id.* The court reasoned that "[e]mployers strive to run their businesses efficiently and they have incentive to protect **employee** information and prevent these types of occurrences." *Id.*

Thus, upon consideration of all of the *Althaus* factors, the Superior Court concluded that the trial court properly found that UPMC owed no duty to **Employees** under Pennsylvania law. Nevertheless, the Superior Court continued to examine whether the economic loss doctrine

applied to bar **Employees'** negligence claim. Reiterating the generalized statement of the doctrine (*i.e.*, that "no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage"), the Superior Court opined that the trial court was correct in noting that the *Bilt-Rite* decision was meant to provide a narrow exception to the doctrine only when the losses result from the reliance on the advice of professionals. *Id.* at 325. The Superior Court further agreed with the trial court that the narrow exception did not apply to this case.⁷ *Id.*

Judge Stabile filed a concurring statement that Judge Olson, the author of the majority opinion, joined. Judge Stabile reasoned that the court's decision declining to find a legal duty should be limited to the facts as alleged in this case. *Id.* at 326 (Stabile, J., concurring). He further reasoned that the balance of the *Althaus* factors may change in favor of **employees** at some point in the future "with the evolution and increased use of" electronic storage of information. *Id.* at 327 (Stabile, J., concurring).

Judge Musmanno wrote a dissenting statement concluding that, on balance, the *Althaus* factors weighed in favor of imposing a duty of reasonable care on UPMC. Specifically, Judge Musmanno challenged the majority's conclusion that the social utility of electronically storing **employee** information outweighed the risk and foreseeability of the harm, believing it to be "untenable, given the ubiquitous nature of electronic data storage, the risk to UPMC's **employees** posed by the failure to reasonably protect such information, and the foreseeability of a computer breach and subsequent identify theft." *Id.* at 328 (Musmanno, J., dissenting). Moreover, Judge Musmanno posited that **Employees'** "assertions, if proven, would establish that UPMC knew or should have realized that inadequate electronic **data** protections would create a likelihood that its **employees'** personal information would be compromised, and that a third party would avail itself of the opportunity to steal this sensitive **data**." *Id.* (Musmanno, J., dissenting). Further, Judge Musmanno reasoned that, "[u]nder the circumstances alleged, the criminal acts of third parties do not relieve UPMC of its duty of care in the protection of [**Employees'**] sensitive personal **data**." *Id.* (Musmanno, J., dissenting).

*5 Judge Musmanno also disagreed with the majority's conclusion that the imposition of a duty of care is unnecessary to incentivize companies to protect their confidential information. Judge Musmanno noted that, while the majority declined to impose a duty due to the significant costs imposed upon employers and the inability to prevent every **data** breach, the *Althaus* test

does not require that the proposed duty prevent all harm.⁸ *Id.* (Musmanno, J., dissenting). Judge Musmanno continued that, when considered against the cost to **employees** resulting from the data breach, the factor relating to the consequences of imposing a duty weighed in favor of imposing a duty. *Id.* (Musmanno, J., dissenting). Finally, Judge Musmanno disagreed with the majority's conclusion that the public interest in imposing a duty weighed in favor of UPMC, opining that, "[w]hile judicial resources may be expended during litigation of data breaches, the public has a greater interest in protecting the personal and sensitive data collected and electronically stored by employers." *Id.* at 328-29 (Musmanno, J., dissenting).

We granted allowance of appeal to address the following issues, as stated by **Employees**:

- a. Does an employer have a legal duty to use reasonable care to safeguard sensitive personal information of its **employees** when the employer chooses to store such information on an internet accessible computer system?
- b. Does the economic loss doctrine permit recovery for purely pecuniary damages which result from the breach of an independent legal duty arising under common law, as opposed to the breach of a contractual duty?

Dittman v. UPMC, — Pa. —, 170 A.3d 1042 (2017) (*per curiam*).

[1] [2] [3] [4] [5] This matter presents pure questions of law, over which our standard of review is *de novo*, and our scope of review is plenary. *Skotnicki v. Insurance Department*, — Pa. —, 175 A.3d 239, 247 (2017). Further, as **Employees'** negligence claim was dismissed on preliminary objections in the nature of a demurrer, we must determine "whether, on the facts averred, the law says with certainty that no recovery is possible." *Bilt-Rite Contractors*, 866 A.2d at 274. Any existing doubt as to whether a demurrer should be sustained should be resolved in favor of overruling it. *Id.* Additionally, we accept as true all material facts as set forth in the complaint and any inferences reasonably deducible therefrom in conducting our review. *Id.* at 272.

A. Duty

Employees contend that, in collecting and storing the

sensitive personal and financial information it required **Employees** to provide, UPMC owed a duty to **Employees** to exercise reasonable care under the circumstances, which includes using reasonable measures to protect the information from the foreseeable risk of a data breach. In support of their position, **Employees** first argue that resort to the *Althaus* factors for purposes of determining the existence of a duty in this case is unnecessary. Specifically, **Employees** argue that the *Althaus* test applies only when determining whether to impose a new, affirmative duty not yet existing under common law, and not when a longstanding preexisting duty arises in a novel factual scenario. **Employees'** Brief at 14-15 (quoting *Alderwoods (Pennsylvania), Inc. v. Duquesne Light Co.*, 630 Pa. 45, 106 A.3d 27, 40 (2014) (explaining that, *inter alia*, the *Althaus* factors are "more relevant to the creation of new duties than to the vindication of existing ones")). **Employees** contend that the trial court and Superior Court erred in treating their claim as one seeking the creation of a new, affirmative duty requiring application of the *Althaus* test, and in concluding that UPMC did not owe a duty. As further explained below, **Employees** claim that they instead seek to impose upon UPMC a duty of care long-established in Pennsylvania law under the novel facts of this case.

*6 In support of their assertion, **Employees** argue that, as a general rule, "anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act." **Employees'** Brief at 17 (quoting Restatement (Second) of Torts § 302, cmt. a (1965)). **Employees** claim that this is a broad expression of duty applicable to many forms of activity, even in novel factual scenarios with no direct precedent such as this one. Applying this broad expression of duty to the facts herein, **Employees** contend that UPMC engaged in the affirmative act of collecting **Employees'** sensitive personal data and storing it on their internet-accessible computer systems. **Employees** maintain that, in so doing, UPMC was under a duty to them to exercise reasonable care under the circumstances, which includes taking reasonable measures to protect them from the foreseeable risk that third parties would attempt to access and pilfer that information. Thus, **Employees** claim that they are alleging misfeasance on behalf of UPMC in collecting and storing **Employees'** sensitive personal data.

Employees further contend that this broad duty is limited by the concept of foreseeability.⁹ With respect to foreseeability, **Employees** argue that troves of electronic data stored on internet-accessible computers held by large entities are obvious targets for cyber criminals and that a reasonable entity in UPMC's position should

foresee that a failure to use basic security measures can lead to exposure of the data and serious financial consequences for the victims. **Employees** thus claim that, in light of the prevalence of electronic data storage in the employment context and the foreseeable risk of breaches of such data, it is appropriate to require employers to use reasonable care when handling and storing **employee data** in order to protect it from compromise. **Employees** argue that there is no sound justification for exempting employers from a duty to act with reasonable care when they collect and store **employees'** sensitive personal information.

Finally, **Employees** contend that the fact that the ultimate harm in this case resulted from criminal activity does not eviscerate the duty UPMC owed to **Employees** to handle its collection and storage of **employee data** with reasonable care. **Employees** acknowledge that one generally does not owe a duty to others to protect them against criminal conduct. **Employees** contend, however, that there are many exceptions to this rule and that the duty to take reasonable anticipatory measures against foreseeable criminal conduct in certain scenarios has deep roots in common law. **Employees'** Brief at 22-24 (relying upon Sections 302 and 302B of the Restatement (Second) of Torts and Comment E thereto, discussed *infra*).

In response, UPMC challenges **Employees'** assertion that it assumed a legal duty to protect against a criminal data breach through commission of an affirmative act. UPMC contends that it merely possessed **employee** information incident to a general employment relationship, which cannot constitute an affirmative act that entails legal liability for third-party criminal conduct. UPMC notes that it is not in the business of providing data security, was not retained to provide data security, was not otherwise tasked with providing data security, and never pursued such an undertaking.

Indeed, according to UPMC, **Employees** are not claiming any affirmative misfeasance on UPMC's part but, rather, nonfeasance in that UPMC failed to prevent the harm incurred or some speculative future harm. In that regard, UPMC notes that there is a "no-duty rule in rescue/protection scenarios where the defendant did not create the risk resulting in harm to the plaintiff." UPMC's Brief at 45 (quoting *Seebold v. Prison Health Services, Inc.*, 618 Pa. 632, 57 A.3d 1232, 1246 (2012)). UPMC contends that "[i]t is nonsensical to suggest that [it] created the risk of harm from a criminal data breach[] simply by possessing **employee data**" and its business neither increased the risk of criminal activity nor posed a special danger to the public regarding unshielded data. *Id.* at 45, 50-51. UPMC contends that third party criminality,

not any affirmative conduct on UPMC's part, created the risk of harm and that it cannot be held liable for an external criminal hack merely because of the general prevalence or conceivable risk of data breaches. UPMC further argues that a third-party criminal act is a superseding cause of the resulting harm and should not be deemed "foreseeable by a negligent actor merely because he or she could have speculated that they might conceivably occur." *Id.* at 51 (citing, *inter alia*, *Ford v. Jeffries*, 474 Pa. 588, 379 A.2d 111, 115 (1977), and *Mahan v. Am-Gard, Inc.*, 841 A.2d 1052, 1061 (Pa. Super. 2003)).

*7 UPMC thus argues that **Employees** "are proposing a radical reconstruction of duty" where they seek to impose liability on UPMC for the criminal acts of unknown third parties. *Id.* at 45. UPMC contends that the decision to impose a legal duty requires a policy determination, made through analysis of the *Althaus* factors, regarding whether a plaintiff is entitled to recover from a defendant for a particular harm on particular facts. UPMC further claims that, as recognized by the courts below, policy considerations do not permit **Employees'** recovery in negligence in this case under both an *Althaus* analysis and the economic loss doctrine, and numerous other jurisdictions have likewise declined to adopt that duty. UPMC contends that, having failed below to establish an exception to the economic loss doctrine or a legal duty under *Althaus*, **Employees** now seek to ignore the requisite policy analysis and instead make the specious claim that UPMC owes them a duty under general negligence principles. UPMC contends that no general rule of negligence can subject them to liability for third-party criminal conduct and claims that to subject all Pennsylvania companies that store **employee data** to liability for criminal data breaches is untenable and against the lower courts' policy determination pursuant to *Althaus* that no such duty be imposed.¹⁰

Having considered the parties' arguments, we agree with **Employees** that this case is one involving application of an existing duty to a novel factual scenario, as opposed to the imposition of a new, affirmative duty requiring analysis of the *Althaus* factors. As **Employees** set forth in their brief, this Court observed in *Alderwoods* that the *Althaus* factors are "more relevant to the creation of new duties than to the vindication of existing ones." *Alderwoods*, 106 A.3d at 40. This Court further explained that it is unnecessary "to conduct a full-blown public policy assessment in every instance in which a longstanding duty imposed on members of the public at large arises in a novel factual scenario. Common-law duties stated in general terms are framed in such fashion for the very reason that they have broad-scale

application.” *Id.* at 40-41; see also *Scampone v. Highland Park Care Center, LLC*, 618 Pa. 363, 57 A.3d 582, 599 (2012) (“Like any other cause of action at common law, negligence evolves through either directly applicable decisional law or by analogy, meaning that a defendant is not categorically exempt from liability simply because appellate decisional law has not specifically addressed a theory of liability in a particular context.”).

As for the common law duty at issue here, this Court has observed that “[i]n scenarios involving an actor’s affirmative conduct, he is generally ‘under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.’” *Seebold*, 57 A.3d at 1246 (quoting Section 302 cmt. a of the Restatement (Second) of Torts). The *Seebold* Court explained that “[t]his duty appropriately undergirds the vast expanse of tort claims in which a defendant’s affirmative, risk-causing conduct is in issue.” *Id.* Indeed, this Court noted that “many judicial opinions on the subject of negligence do not specifically address the duty element,” not because they “fail to see duty as an element of negligence, but because they presume the existence of a duty where the defendant’s conduct created a risk.” *Id.* at 1246 n.21 (quoting *Cardi & Green, Duty Wars*, 81 S. CAL. L. REV. 671, 702 (2008)).

*8 ^[6] ^[7] **Employees** have alleged and, as the case is before us at the preliminary objection stage, we currently must accept as true that, as a condition of employment, UPMC required them to provide certain personal and financial information, which UPMC collected and stored on its internet-accessible computer system without use of adequate security measures, including proper encryption, adequate firewalls, and an adequate authentication protocol. These factual assertions plainly constitute affirmative conduct on the part of UPMC. Additionally, while UPMC is correct that, generally, “there is no duty to protect or rescue someone who is at risk on account of circumstances the defendant had no role in creating,” *id.* at 1246, **Employees** have sufficiently alleged that UPMC’s affirmative conduct created the risk of a data breach. Thus, we agree with **Employees** that, in collecting and storing **Employees’** data on its computer systems, UPMC owed **Employees** a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act.

^[8] ^[9] Further, to the extent that UPMC argues that the presence of third-party criminality in this case eliminates the duty it owes to **Employees**, we do not agree. As stated above, UPMC relies on selected portions of *Ford* and *Mahan* in support of its position that it cannot be liable for third-party criminal conduct that could “conceivably

occur.” However, as *Ford* more fully outlined:

The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although the actor’s negligent conduct created a situation which afforded an opportunity to the third person to commit such a tort or crime, unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime.

Ford, 379 A.2d at 115 (quoting Section 448 of the Restatement (Second) of Torts (1965)).¹¹ Further, while the Superior Court in *Mahan* observed that “the wrongful actions of a third party are not deemed to be foreseeable by a negligent actor merely because he or she could have speculated that they might conceivably occur,” the court, citing *Jeffries*, acknowledged that liability could be found if the actor “realized or should have realized the likelihood that such a situation might be created and that a third person might avail himself of the opportunity to commit such a tort or crime.” *Mahan*, 841 A.2d at 1061.¹²

*9 Again, **Employees** allege that UPMC, their employer, undertook the collection and storage of their requested sensitive personal data without implementing adequate security measures to protect against data breaches, including encrypting data properly, establishing adequate firewalls, and implementing adequate authentication protocol. The alleged conditions surrounding UPMC’s data collection and storage are such that a cybercriminal might take advantage of the vulnerabilities in UPMC’s computer system and steal **Employees’** information; thus, the data breach was “within the scope of the risk created by” UPMC. See *Ford*, 379 A.2d at 115 (explaining that the dilapidated condition of the appellee’s property, which had caught fire and damaged the appellant’s neighboring property, “was such that third persons might avail themselves of the opportunity to commit a tort or crime” and that “such acts were within the scope of the risk created by the appellee”). Therefore, the criminal acts of third parties in executing the data breach do not alleviate UPMC of its duty to protect **Employees’** personal and financial information from that breach.

Based on the foregoing, we conclude that the lower courts erred in finding that UPMC did not owe a duty to **Employees** to exercise reasonable care in collecting and storing their personal and financial information on its computer systems. This conclusion notwithstanding, **Employees'** claim cannot proceed if we nonetheless hold that it is barred by the economic loss doctrine. Thus, we turn to our analysis of that doctrine.

B. The Economic Loss Doctrine

The crux of the dispute before us is whether the economic loss doctrine as applied in Pennsylvania precludes all negligence claims that seek to recover for purely economic damages, save for specifically delineated and narrow exceptions, or whether such claims are generally permitted provided that a plaintiff can establish a breach of a legal duty independent of any contractual duties existing between the parties. As evidenced throughout this opinion, much of the dispute in this regard centers on the proper interpretation of our decisions in *Bilt-Rite* and *Excavation Technologies*, which form the basis of the parties' arguments and which we analyze in further detail below.

Beginning with the parties' contentions, **Employees** argue that courts have incorrectly read our decision in *Bilt-Rite* as merely permitting negligent misrepresentation claims under Section 552 of the Restatement (Second) of Torts, *see infra* at pages ——— n.17, as a narrow exception to an otherwise broad economic loss doctrine precluding all negligence claims for solely monetary harm. **Employees** claim that, under *Bilt-Rite*, the economic loss doctrine does not bar negligence-based tort claims involving purely financial harm, provided that the plaintiff establishes that the defendant owed a common law duty arising independently from any contract between the parties. **Employees** argue that the holding in *Bilt-Rite* did not rely or otherwise depend upon the particular legal duty imposed or tort alleged in that case and therefore was not limited in that manner.

Employees contend that *Bilt-Rite's* iteration of the rule as they believe it should be interpreted is more coherent and precise than the general statement of the rule, "which fails to explain or reconcile a plethora of obvious 'exceptions.'" **Employees'** Brief at 51. **Employees** further argue that their interpretation of the doctrine, which focuses on the source of the duty, is consistent with the definition accepted by many states and scholars, and will reduce

confusion and unjust deployment of the rule against legitimate tort claims while serving the rule's purpose of precluding those claims that seek to compensate parties for losses resulting from a breach of contractual duties. **Employees** thus contend that, here, we need only to reaffirm *Bilt-Rite's* enunciation of the rule as stated by them and hold that it does not bar their negligence claim.

UPMC counters that the lower courts correctly held that the economic loss doctrine precludes **Employees'** negligence claim for monetary damages.¹³ UPMC argues that the economic loss doctrine is well-settled in Pennsylvania and broadly applies to bar negligence claims that result "solely in economic damages unaccompanied by physical injury or property damage." UPMC's Brief at 12, 14-15 (quoting *Excavation Technologies, Inc.*, 985 A.2d at 841 n.3). Relying upon *Excavation Technologies*, UPMC further interprets *Bilt-Rite's* holding as creating a narrow exception to the broad economic loss doctrine for negligent misrepresentation claims under Section 552 of the Restatement (Second) of Torts that involve design professionals supplying information to others for pecuniary gain. UPMC claims that no Pennsylvania court has applied **Employees'** interpretation of *Bilt-Rite* in an action to recover purely economic damages under a common law negligence theory and argues that this Court already declined to expand *Bilt-Rite* in the manner **Employees** suggest in *Excavation Technologies*.

*10 UPMC also claims that **Employees**, focusing upon "misleading dicta" in *Bilt-Rite*, argue for an improperly expansive interpretation of that case which would effectively render the economic loss doctrine a nullity by exempting all common law negligence claims from its application.¹⁴ *Id.* at 16-18. UPMC contends that the language **Employees** rely upon from *Bilt-Rite* in support of their position "merely recognizes an uncontroversial aspect of tort law": that "financial damages may be recoverable under several specific torts [that include] financial detriment ... as an element of the tort itself." *Id.* at 18. UPMC argues that **Employees'** failure to distinguish between common law negligence and specific tort claims highlights the error in their argument.

UPMC argues that **Employees'** "tortured construction" of the economic loss doctrine "distills to the untenable proposition that our appellate courts have misconstrued the rule since its inception" and that accepting **Employees'** position would contravene the doctrine's purpose of preventing indeterminate liability. *Id.* at 12-13, 16 n.4. UPMC further maintains that the Third Circuit has already considered and rejected **Employees'** arguments regarding the contours of Pennsylvania's economic loss

doctrine and *Bilt-Rite's* holding, including in the context of computer information theft. *Id.* at 18-20 (citing, *inter alia*, *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 178 (3d Cir. 2008) (opining that this Court in *Bilt-Rite* "simply carved out a narrow exception [to the economic loss doctrine] when losses result from the reliance on the advice of professionals")). Additionally, UPMC claims that a majority of jurisdictions confronting data breach litigation have dismissed negligence claims in accord with the economic loss doctrine.^{15,16}

*11 As the parties' arguments focus on this Court's decisions in *Bilt-Rite* (2005) and *Excavation Technologies* (2009), we begin with a summary of those cases. In *Bilt-Rite*, East Penn School District (District) entered into a contract with The Architectural Studio (TAS) for architectural services related to the design and construction of a new school. These services included the preparation of plans, drawings, and specifications that would be submitted to contractors for the purpose of preparing bids for the new school's construction. The District solicited bids from contractors for the project, including TAS's plans, drawings, and specifications in the bid documents supplied to the contractors. The District eventually awarded the contract to Bilt-Rite Contractors, Inc. (Bilt-Rite), and the District and Bilt-Rite entered into a contract for the project. The contract specifically referred to and incorporated by reference the plans, drawings, and specifications from TAS.

As part of the project, TAS's plans provided for the installation of certain systems that TAS "expressly represented could be installed and constructed through the use of normal and reasonable construction means and methods, using standard construction design tables." *Bilt-Rite*, 866 A.2d at 272. However, once Bilt-Rite began the work, it discovered that construction of the systems required it to employ special construction means, methods, and design tables, resulting in substantially increased construction costs. It thus "sued TAS on a theory of negligent misrepresentation under Section 552 of the Restatement (Second) of Torts,¹⁷ claiming that TAS's specifications were false and/or misleading, and seeking damages for its increased construction costs." *Id.* at 272-73. TAS filed preliminary objections in the nature of a demurrer, arguing that "the economic loss doctrine," which holds that a tort plaintiff cannot recover for purely economic losses" barred *Bilt-Rite's* action and that TAS did not owe a duty to Bilt-Rite, with whom it had no contractual relationship. *Id.* at 273. The trial court sustained TAS's preliminary objections, and the Superior Court affirmed.

On appeal, this Court was presented with the issue of

"whether a building contractor may maintain a negligent misrepresentation claim against an architect for alleged misrepresentations in the architect's plans for a public construction contract, where there was no privity of contract between the architect and the contractor, but the contractor reasonably relied upon the misrepresentations in submitting its winning bid and consequently suffered purely economic damages as a result of that reliance." *Id.* at 272. In addressing that issue, this Court formally adopted Section 552 of the Restatement (Second) of Torts as the law in Pennsylvania for negligent misrepresentation claims involving those in the business of supplying information to others, such as an architect or design professional.¹⁸ *Id.* at 287. The Court noted that recovery was possible even if the third party had no direct contractual relationship with the supplier of the information, as "Section 552 negates any requirement of privity." *Id.*

*12 Most importantly for our current purposes, with respect to application of the economic loss doctrine, the Court looked to the "reasoned approach to the rule" expressed by the South Carolina Supreme Court in *Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc.*, 320 S.C. 49, 463 S.E.2d 85 (1995), which observed that its

application of the "economic loss" rule maintains the dividing line between tort and contract while recognizing the realities of modern tort law. Purely "economic loss" may be recoverable under a variety of tort theories. The question, thus, is not whether the damages are physical or economic. Rather, the question of whether the plaintiff may maintain an action in tort for purely economic loss turns on the determination of the source of the duty plaintiff claims the defendant owed. A breach of a duty which arises under the provisions of a contract between the parties must be redressed under contract, and a tort action will not lie. A breach of duty arising independently of any contract duties between the parties, however, may support a tort action.

Id. at 287-88 (quoting *Tommy L. Griffin Plumbing*, 463 S.E.2d at 88 (footnote and citation omitted)). The *Tommy L. Griffin Plumbing* Court listed libel and defamation, accountant malpractice, legal malpractice, and architect

liability among the examples of tort actions for which purely economic loss is recoverable. *Tommy L. Griffin Plumbing*, 463 S.E.2d at 88 & n.2.

This Court in *Bilt-Rite* explained that, “[l]ike South Carolina, Pennsylvania has long recognized that purely economic losses are recoverable in a variety of tort actions including the professional malpractice actions noted by the South Carolina Supreme Court.” *Bilt-Rite Contractors*, 866 A.2d at 288. It thus agreed that “a plaintiff is not barred from recovering economic losses simply because the action sounds in tort rather than contract law.” *Id.* In so doing, the Court noted that Bilt-Rite had no contractual relationship with TAS and thus, recovery under a contract theory was unavailable. However, because Bilt-Rite stated a viable claim for negligent misrepresentation under Section 552, which did not require privity, “logic dictate[d] that Bilt-Rite not be barred from recovering the damages it incurred, if proven.”¹⁹ *Id.* The Court therefore held that the economic loss doctrine was inapplicable to negligent representation claims arising under Section 552. *Id.*

Following *Bilt-Rite*, this Court decided *Excavation Technologies*. In that case, Excavation Technologies, Inc. (Excavation Technologies) requested that Columbia Gas Company of Pennsylvania (Columbia) mark the locations of gas lines around work sites pursuant to the One Call Act.²⁰ Columbia improperly marked some lines and failed to mark others, resulting in Excavation Technologies striking various gas lines, which in turn hampered its work and caused it economic damages. Based on the foregoing, Excavation Technologies sued Columbia on a theory of negligent misrepresentation under Section 552 of the Restatement (Second) of Torts, alleging that Columbia failed to comply with its duties under the One Call Act. In response, Columbia filed preliminary objections in the nature of a demurrer, claiming that the economic loss doctrine precluded liability. The trial court sustained Columbia’s preliminary objections, and the Superior Court affirmed.

*13 This Court granted review to decide “whether [Section] 552 of the Restatement (Second) of Torts [see *supra* at pages — — — n.17] imposes liability for economic losses to a contractor caused when a gas utility company fails to mark or improperly marks the location of gas lines.” *Excavation Technologies*, 985 A.2d at 842. In answering this question, the Court distinguished the case from *Bilt-Rite* on the basis that Columbia was “not in the business of providing information for pecuniary gain” and therefore concluded that Section 552(1) and (2) of the Restatement (Second) of Torts were inapplicable. *Id.* at 843. Additionally, the Court declined Excavation

Technologies’ invitation to impose liability under Section 552(3) of the Restatement (Second) of Torts, which was not at issue and thus not addressed by *Bilt-Rite*. The Court rejected the argument that Section 552(3) applied because Columbia was under a duty to provide accurate information as to the location of its underground lines. In support of its conclusion, the Court reasoned that: (1) the Act’s purpose was to protect against physical harm and property damage, not economic losses; (2) excavators, and not utility companies, ultimately retained the duty to identify the precise location of facilities pursuant to the Act; and (3) public policy weighed against imposing liability, as the costs would inevitably be passed to the consumer if utility companies were exposed to liability for an excavators’ economic losses.²¹ *Id.* at 844.

In addition to its analysis above, the Court concluded that there was no statutory basis to impose liability for economic losses. It is at this point the Court discussed the economic loss doctrine, which the Court previously defined in a footnote as providing that “no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage.” *Id.* at 841 n.3 (quoting *Adams v. Copper Beach Townhome Communities, L.P.*, 816 A.2d 301, 305 (Pa. Super. 2003)). The Court reasoned that the “economic loss doctrine was well-established in tort law when the [One Call] Act was enacted” and later amended. *Id.* at 842 (citing *Aikens v. Baltimore and Ohio Railroad Co.*, 348 Pa. Super. 17, 501 A.2d 277 (1985), which noted that the roots of the economic loss doctrine were first recognized in *Robins Dry Dock & Repair Co. v. Flint*, 275 U.S. 303, 48 S.Ct. 134, 72 L.Ed. 290 (1927)). The Court continued by explaining that “[t]he legislature was presumably aware of the economic loss doctrine when it established the statutory scheme governing the relationship among the entities required to participate under the Act,” and found that “our legislature did not intend utility companies to be liable for economic harm caused by an inaccurate response under the Act, because it did not provide a private cause of action for economic losses.” *Id.* at 842-43. In the context of this discussion, the Court cited *In re Rodriguez*, 587 Pa. 408, 900 A.2d 341, 345 (2003), for the proposition that “courts must assume [that the] legislature understands [the] legal landscape on which it enacts laws, and when [the] common law rule is not abrogated, they must assume it persists.” *Id.* at 843.

^[10] Having set forth our decisions in *Bilt-Rite* and *Excavation Technologies*, we hold that those cases do not stand for the proposition that the economic loss doctrine, as applied in Pennsylvania, precludes all negligence claims seeking solely economic damages. Indeed, the *Bilt-Rite* Court unequivocally stated that “Pennsylvania

has long recognized that purely economic losses are recoverable in a variety of tort actions” and that “a plaintiff is not barred from recovering economic losses simply because the action sounds in tort rather than contract law.” *Bilt-Rite*, 866 A.2d at 288. In so doing, the Court set forth a “reasoned approach” to applying the economic loss doctrine that “turns on the determination of the source of the duty plaintiff claims the defendant owed.” *Id.* (quoting *Tommy L. Griffin Plumbing*, 463 S.E.2d at 88). Specifically, if the duty arises under a contract between the parties, a tort action will not lie from a breach of that duty. However, if the duty arises independently of any contractual duties between the parties, then a breach of that duty may support a tort action. *Id.*

*14 As stated above, the *Bilt-Rite* Court took this approach from the Supreme Court of South Carolina in the case of *Tommy L. Griffin Plumbing*. Notably, in *Tommy L. Griffin Plumbing*, the Supreme Court of South Carolina observed that “some states use the ‘economic loss’ rule to prohibit all recovery of purely economic damages in tort.” *Tommy L. Griffin Plumbing*, 463 S.E.2d at 88. The South Carolina Supreme Court, however, rejected that approach in light of the fact that “[t]he law in South Carolina ... has long recognized tort actions when the damages are purely economic.” *Id.* at 88 & n.2 (citing cases involving tort actions for purely economic damages, including architect liability, legal malpractice, accountant malpractice, and libel and defamation). In recognizing that Pennsylvania similarly “has long recognized that purely economic losses are recoverable in variety of tort actions,” *Bilt-Rite*, 866 A.2d at 288, and accepting South Carolina’s annunciation of the economic loss doctrine, this Court likewise rejected that approach.

As for UPMC’s argument that *Bilt-Rite* merely created a narrow exception to the otherwise broad economic loss doctrine for negligent misrepresentation claims falling under Section 552 of the Restatement, we find that argument unpersuasive. The *Bilt-Rite* Court set forth the general approach to the economic loss doctrine as gleaned from the South Carolina Supreme Court above and noted that Pennsylvania permits recovery of purely economic losses in a variety of tort actions. The *Bilt-Rite* Court concluded that, because *Bilt-Rite* had stated a viable claim for negligent misrepresentation under Section 552 of the Restatement, the economic loss doctrine did not bar its claim. In other words, *Bilt-Rite* held that a negligent misrepresentation claim made under Section 552 of the Restatement is one among many tort claims in Pennsylvania for which the economic loss doctrine does not act as a bar for recovery of purely economic losses.

Our reading of *Excavation Technologies* does not compel a different conclusion. As noted, the issue in that case was whether, under a theory of negligent misrepresentation pursuant to Section 552 of the Restatement (Second) of Torts, a utility is liable to a contractor for economic losses sustained when the utility fails to mark or improperly marks the location of gas lines pursuant to the One Call Act. In deciding that issue in the negative, the Court held that the contractor’s claim did not fall under Section 552(1) and (2) of the Restatement (Second) of Torts and declined to impose liability under Section 552(3) of the Restatement. Thus, the *Excavation Technologies* Court did not hold that the economic loss doctrine barred *Excavation Technologies*’ claim. Rather, it held that *Excavation Technologies* failed to state a viable claim for negligent misrepresentation under Section 552 of the Restatement in the first instance.

We acknowledge that the *Excavation Technologies* Court concluded that there was no statutory basis to impose liability on utility companies for economic losses under the One Call Act and, in so doing, included a broad definition and brief discussion of the economic loss doctrine. However, we find these observations to be ancillary not only to the Court’s conclusion that the One Call Act did not provide for recovery of economic losses, but also to the Court’s central holding that, in contrast to *Bilt-Rite*, the contractor failed to state a claim for negligent misrepresentation under Section 552 under the Restatement. Further, the Court supported its comments on the economic loss doctrine by citing nonbinding cases from the Superior Court that pre-date this Court’s approach to the doctrine in *Bilt-Rite*. See *Excavation Technologies*, 985 A.2d at 841-43 & n.3 (quoting *Adams*, 816 A.2d at 305, and citing *Aikens*, 501 A.2d at 278-79).²² Indeed, the *Excavation Technologies* Court did not discuss *Bilt-Rite*’s approach to the doctrine, set forth above, at all. Thus, to the extent *Excavation Technologies* can be interpreted as having any impact on the Court’s expression of the rule under *Bilt-Rite* as we have now reaffirmed, we reject that interpretation.

*15 ^[11]Here, **Employees** have asserted that UPMC breached its common law duty to act with reasonable care in collecting and storing their personal and financial information on its computer systems. As this legal duty exists independently from any contractual obligations between the parties, the economic loss doctrine does not bar **Employees**’ claim.

D. Conclusion

Based on the foregoing, we conclude that the courts below erred in determining that UPMC did not owe a duty to **Employees** to use reasonable care to safeguard their sensitive personal data in collecting and storing it on an internet-accessible computer system. We further hold that the lower courts erred in concluding that Pennsylvania's economic loss doctrine bars **Employees'** negligence claim. Accordingly, we vacate the judgment of the Superior Court, reverse the order of the trial court, and remand the matter to the trial court for further proceedings consistent with this opinion.

Justices Dougherty, Wecht and Mundy join the opinion.

Chief Justice Saylor files a concurring and dissenting opinion in which Justice Todd joins.

Justice Donohue did not participate in the consideration or decision of this matter.

CHIEF JUSTICE SAYLOR, Concurring and Dissenting

I agree with the majority that **Employees'** negligence claim should not have been dismissed upon a demurrer, at the preliminary objection stage, contesting the legal sufficiency of the complaint. I respectfully differ, however, with material aspects of the majority's reasoning.

From my point of view, the claim in issue sounds in both contract and tort, thus presenting a hybrid scenario. In this regard, **Employees'** claim is expressly premised on the discrete relationship between employers and **employees** relative to confidential personal and financial information provided *as a condition of employment*. See Second Amended Class Action Complaint at ¶ 56. This suggests that the claim should be viewed through a contract lens. Nevertheless, Section 302B of the Second Restatement -- addressing the risk of intentional or criminal acts -- recognizes that duties arising out of contractual relationships may form the basis for tort liabilities. See Restatement (Second) § 302B, cmt. e (1965) ("There are ... situations in which the actor, as a reasonable man, is required to anticipate and guard against the intentional, or even criminal, misconduct of others[,] ... including "[w]here, by contract or otherwise, the actor has undertaken a duty to protect the other against such misconduct"). See generally *Snoparsky v. Baer*, 439 Pa. 140, 145-46, 266 A.2d 707, 710 (1970) (referencing

Section 302B favorably).¹

Ultimately, I find that an employer who collects confidential personal and financial information from **employees** stands in such a special relationship to those **employees** with respect to that information, and I have no difficulty concluding that such a relationship should give rise to a duty of reasonable care to ensure the maintenance of appropriate confidentiality as against reasonably foreseeable criminal activity.²

*16 This brings me to the economic loss doctrine. Initially, I respectfully differ with the majority's position that the doctrine should be essentially removed from the tort arena so long as the duty involved can be categorized as "existing independently from any contractual obligations between the parties." Majority Opinion, at --- -- ---.³ In this regard, I note that the economic loss doctrine serves as a bulwark against uncontrolled liability. See, e.g., *Ultramares Corp. v. Touche*, 255 N.Y. 170, 174 N.E. 441, 444 (1931) (Cardozo, C.J.) (warning against imposing liability "an indeterminate amount for an indeterminate time to an indeterminate class"). See generally Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 348-60 (2017) (depicting the application of the economic loss rule in the "stranger paradigm," where the actor has no preexisting contractual or special relationship with an injured victim). From my point of view, a proclamation negating the operation of the economic loss doctrine in the tort law arena is both unnecessary to the resolution of the present case and imprudent. Instead, particularly because of the hybrid nature of **Employees'** claim, I find that the applicability of the economic loss doctrine should be determined more by way of a discrete social policy assessment than as a matter of mere categorization.⁴

In this regard, I am sympathetic to UPMC's concerns about exposure to litigation and the scale of the potential liability involved. Nevertheless, I would also be reluctant to hold that employers should be absolutely immune from liability for any sort of economic damages occasioned by negligent conduct on their part relative to the safeguarding of confidential personal and financial data. Along these lines, I note that some other courts have applied the economic loss doctrine to impose limitations on the scope of damages without foreclosing economic damages entirely. See, e.g., *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162 (1st Cir. 2011) (discussing the availability, in Maine, of recovery for economic losses in the form of "mitigation damages," i.e., recovery for costs and harms incurred during a reasonable effort to mitigate losses occasioned by computer data breaches). Although

any such limitations are not directly in issue here, I strike the balance here in favor of permitting recovery of at least mitigation damages -- in the **data** breach context -- in instances in which an **employee** or **employees** prove that the employer has violated the duty to exercise reasonable care in protecting confidential personal and financial **data**.⁵

*17 Finally, I appreciate that this matter of substantive tort law is more properly the domain of the Legislature. Nevertheless, I agree with the majority -- in the broadest frame -- that a pre-existing, traditional tort framework can be applied to the claim involved, and, again, I find that the economic loss doctrine, and other rational constraints, can be assessed in terms of the damages calculation for proven, wrongful conduct on an employer's part.⁶

In summary, while I concur in the majority's determination that Count I of the complaint should be reinstated, I respectfully dissent concerning the legal principles by which the majority undertakes to curtail the economic loss doctrine.

Justice Todd joins this concurring and dissenting opinion.

All Citations

--- A.3d ----, 2018 WL 6072199

Footnotes

- 1 **Employees** brought their claims on behalf of two separate but overlapping classes of similarly situated persons: (1) current and former UPMC **employees** whose personal and financial information was stolen and "used to file fraudulent tax returns or otherwise misused in a manner which resulted in financial harm," and (2) current and former UPMC **employees** whose personal and financial information was stolen and "who are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse as a result of the [d]ata [b]reach." Second Amended Class Action Complaint, 6/25/2014, at ¶ 39.
- 2 In *Althaus*, this Court observed:
The determination of whether a duty exists in a particular case involves the weighing of several discrete factors which include: (1) the relationship between the parties; (2) the social utility of the actor's conduct; (3) the nature of the risk imposed and foreseeability of the harm incurred; (4) the consequences of imposing a duty upon the actor; and (5) the overall public interest in the proposed solution.
Althaus, 756 A.2d at 1169.
- 3 The court also dismissed **Employees'** breach of implied contract claim on preliminary objections. That claim is not at issue in this appeal.
- 4 As later discussed in detail, *Bilt-Rite* involved a contractor's claim for negligent misrepresentation under Section 552 of the Restatement (Second) of Torts, *infra* at pages ---- -- ---- n.17, against an architectural firm that had provided plans to a school district for use in soliciting bids for a construction project. *Bilt-Rite*, 866 A.2d at 272-73. The contractor alleged that, due to misrepresentations in the plans, which it had ultimately incorporated into its construction contract with the school district upon winning the bid for the project, it incurred substantial extra costs in performing the work. *Id.* This Court concluded that the economic loss doctrine did not bar the contractor's claim. *Id.* at 288.
- 5 In this regard, the trial court found a decision from the Appellate Court of Illinois, *Cooney v. Chicago Public Schools*, 407 Ill.App.3d 358, 347 Ill.Dec. 733, 943 N.E.2d 23 (2010), to be persuasive. There, the personal information of more than 1,700 former Chicago Public School **employees** had been disclosed via a mailing that was sent to each of the former **employees**. The court rejected the argument that it "should recognize a 'new common law duty' to safeguard information" that had been disclosed. *Id.*, 347 Ill.Dec. 733, 943 N.E.2d at 28. The court explained that the plaintiffs failed to cite any Illinois case law to support their argument and that the legislature had already addressed the issue via statute, which imposed a duty to provide notice of the disclosure only. The court did not believe that creating "a new legal duty beyond legislative requirements already in place is part of [its] role on appellate review." *Id.*, 347 Ill.Dec. 733, 943 N.E.2d at 29.
- 6 In focusing on risk and foreseeability in a general sense, the Superior Court noted that **Employees** failed to allege that UPMC encountered a specific threat of a **data** breach. *Dittman*, 154 A.3d at 323-24 & n.4.
- 7 This agreement notwithstanding, the Superior Court relied upon *Bilt-Rite* to posit further that, for **Employees** to recover for economic loss alone, they must show that UPMC breached a duty imposed by law, but that no such duty existed here. *Dittman*, 154 A.3d at 325. The court explained that, "[w]ithout a duty imposed by law or a legally recognized

special relationship, the economic loss doctrine bars [Employees'] claims." *Id.*

- 8 Judge Musmanno also criticized the majority's observation that there were statutes and safeguards in place to prevent employers from disclosing confidential information, presumably because this case did not involve the employer itself disclosing the information. *Dittman*, 154 A.3d at 328 (Musmanno, J., dissenting).
- 9 **Employees** also claim that common law duties can be limited in rare instances in light of public policy concerns, but those concerns are best addressed through legislative action. **Employees'** Brief at 18 (citing, *inter alia*, *Alderwoods*, 106 A.3d at 39-40 (explaining that determinations as to immunity from common law tort liability are better suited for the Legislature, which is "better positioned to make informed policymaking judgments").
- 10 Prior to reaching our analysis, we note that both parties also provide argument in their briefs as to whether a common law duty of care exists under the circumstances of this case in light of the Legislature's enactment of the **Data Breach Act**. Briefly, **Employees** argue that, in imposing only a duty of notification of a **data** breach, the **Data Breach Act** does not address, let alone preclude, the existence of a common law duty to act with reasonable care in collecting and storing **data** for the purpose of preventing a breach in the first place. In contrast, UPMC argues against the imposition of a common law duty on the basis that, through enactment of the **Data Breach Act**, the Legislature has conducted a comprehensive assessment of **data** breaches and determined that entities that suffer a **data** breach have a duty only to provide notice of the disclosure of personal information. Upon review of the act, we agree with **Employees** that, in requiring an entity to provide notification of a **data** breach, the act has no bearing on whether an entity has an initial duty under common law to exercise reasonable care to protect **data** prior to a breach. Thus, we find any further discussion of the **Data Breach Act** to be unnecessary with respect to the issue of duty before us.
- 11 See also Restatement (Second) of Torts Section 302 ("A negligent act or omission may be one which involves an unreasonable risk of harm to another through ... the foreseeable action of the other [or] a third person...."); Section 302B ("An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal."), and Comment E thereto (providing that situations exist "in which the actor, as a reasonable man, is required to anticipate and guard against the intentional, or even criminal, misconduct of others" and that, generally, these situations arise "where the actor is under a special responsibility toward the one who suffers the harm, which includes the duty to protect him against such intentional misconduct; or where the actor's own affirmative act has created or exposed the other to a recognizable high degree of risk of harm through such misconduct, which a reasonable man would take into account"). Comment E further sets forth a non-exhaustive list of these situations, including "[w]here the actor stands in such a relation to the other that he is under a duty to protect him against such misconduct ... [such as] employer and employee," and "[w]here property of which the actor has possession or control affords a peculiar temptation or opportunity for intentional interference likely to cause harm." Section 302B of the Restatement (Second) of Torts Cmt. e(B), (G).
- 12 In support of its position that it cannot be held liable for the criminal acts of third parties, UPMC also relies upon *Feld v. Merriam*, 506 Pa. 383, 485 A.2d 742 (1984), for the proposition that "absent agreement, a landlord has no general duty to protect tenants against third-party criminal conduct." UPMC's Brief at 51. *Feld*, however, did not involve the situation where the landlord's conduct created the risk of injury from the criminal acts of third parties. *Feld*, 485 A.2d at 746 (explaining that "the risk of injury from the criminal acts of third persons arises not from the conduct of the landlord but from the conduct of an unpredictable independent agent," and contrasting that circumstance from the risk of injury from a physical defect in the property, where "the landlord has effectively perpetuated the risk of injury by refusing to correct a known and verifiable defect").
- 13 The Pennsylvania Defense Institute, Chamber of Commerce of the United States of America, and Pennsylvania Chamber of Business and Industry have filed an *amici curiae* brief in support of UPMC, where they advance and expand upon the arguments set forth by UPMC regarding the economic loss doctrine as discussed *infra*. In so doing, *amici* add that a majority of jurisdictions apply the economic loss doctrine broadly to bar all negligence claims that cause only economic loss and that the *Bilt-Rite* "exception" is also widely followed.
- 14 UPMC also argues, apparently in the alternative, that **Employees** are improperly attempting to fit their cause of action within the narrow exception created by *Bilt-Rite*, which does not apply to this case, as the lower courts concluded. In their reply brief, **Employees** note that they are not attempting to fit this case into any alleged "Section 552 exception" and that they have never disputed that *Bilt-Rite*'s holding as it relates to Section 552 is inapplicable to this case. **Employees'** Reply Brief at 1-2.
- 15 In their reply brief, **Employees** argue that, *inter alia*, UPMC misconstrues various cases in support of its position, including *Bilt-Rite* and *Excavation Technologies*, and misapprehends the economic loss doctrine as well as the


purpose behind it.

- 16 We further note that, as we similarly commented with respect to the issue of duty in footnote 10, *supra* at page —, the parties provide argument regarding the impact of the Legislature's enactment of the Data Breach Act on application of the economic loss doctrine in this case. UPMC claims that, because the Data Breach Act does not provide a private cause of action for economic losses, but instead established an enforcement action reserved exclusively for the Attorney General for violations of the notification requirement, applying the economic loss doctrine to bar this case is consistent with the actions of the Legislature in enacting the Data Breach Act. UPMC's Brief at 21-24 (relying upon *Excavation Technologies*, 985 A.2d at 842 (finding "it apparent our legislature did not intend utility companies to be liable for economic harm caused by an inaccurate response under the [One Call] Act, [see *infra* at page — n.20.] because it did not provide a private cause of action for economic losses")). In response, **Employees** distinguish *Excavation Technologies* by noting that the duty in that case was statutorily imposed and, thus, the Court properly looked to the One Call Act in analyzing whether an entity could be liable for economic losses. **Employees'** Reply Brief at 13-14. As we concluded with respect to the issue of duty above, we likewise conclude that the Data Breach Act's failure to provide for a private cause of action for economic damages based upon a violation of the statutory duty to provide notification has no impact on the issue of whether a plaintiff can recover solely economic damages under a common law negligence theory for a defendant's initial failure to protect information from a data breach. Thus, no further discussion of the Data Breach Act is necessary as it relates to application of the economic loss doctrine under the circumstances of this case.
- 17 Section 552, titled "Information Negligently Supplied for the Guidance of Others," provides:
- (1) One who, in the course of his business, profession or employment, or in any other transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.
 - (2) Except as stated in Subsection (3), the liability stated in Subsection (1) is limited to loss suffered
 - (a) by the person or one of a limited group of persons for whose benefit and guidance he intends to supply the information or knows that the recipient intends to supply it; and
 - (b) through reliance upon it in a transaction that he intends the information to influence or knows that the recipient so intends or in a substantially similar transaction.
 - (3) The liability of one who is under a public duty to give the information extends to loss suffered by any of the class of persons for whose benefit the duty is created, in any of the transactions in which it is intended to protect them.
- As discussed in further detail below, Section 552(3) was not at issue in *Bilt-Rite*.
- 18 The Court emphasized that, in adopting Section 552, it was not supplanting the common law tort of negligent misrepresentation, but rather "clarifying the contours of the tort as it applies to those in the business of providing information to others." *Bilt-Rite*, 866 A.2d at 287.
- 19 The Court additionally observed that application of the economic loss doctrine in the context of a claim arising under Section 552 would be "nonsensical," as it would allow a party to pursue a cause of action, but preclude recovery for its losses once the elements were demonstrated. *Bilt-Rite Contractors*, 866 A.2d at 288.
- 20 73 P.S. §§ 176-86. The One Call Act requires facility owners to mark the position of underground lines upon request. *Id.* at § 177(5)(i).
- 21 On the last point, the Court noted that "if this is to be done, the legislature will say so specifically" and that "[u]ntil that day, we decline to afford heightened protection to the private interests of entities who are fully capable of protecting themselves, at the public's expense." *Excavation Technologies*, 985 A.2d at 844.
- 22 A brief discussion of *Aikens* and *Adams* is warranted. In *Aikens*, the Superior Court rejected a negligence claim made by **employees** of a manufacturing plant against a railroad company for lost wages resulting from the plant's curtailed production due to damage caused by a train derailment. The Superior Court adopted Section 776C of the Restatement (Second) of Torts, which bars recovery of purely economic damages for negligent interference with a contract or a prospective contractual relation, and concluded that recovery is only possible if the tortious interference is intentional or involved parties in a special relationship to one another. *Aikens*, 501 A.2d at 278-79. Exhibiting a clear concern with foreseeability and limitation of liability, the court supported its conclusion by reasoning that, *inter alia*, "the negligent actor has no knowledge of the contract or prospective relation and thus has no reason to foresee any harm to the plaintiff's interest" and that "[t]o allow a cause of action for negligent cause of purely economic loss would be to open the door to every person in the economic chain of the negligent person or business to bring a cause of action." *Id.* at 279.
- Similarly, in *Adams*, the Superior Court rejected a claim for lost wages and benefits made under the Storm Water

Management Act (SWMA), 32 P.S. §§ 680.1-680.17, by **employees** of a manufacturing plant against entities that owned properties adjacent to the plant, based upon the plant's temporary closure due to storm water runoff from a neighboring property. The Superior Court held that lost wages and benefits did not fall within the scope of the term "injury" as used in the SWMA. *Adams*, 816 A.2d at 307. Though discussion of the economic loss doctrine was ancillary to its conclusion that the **employees** had no statutory basis for relief (as we similarly observed above with respect to *Excavation Technologies*), the court relied upon *Aikens* to explain that the term "injury" as used by the SWMA is analogous to the 'physical injury or property damage' requirements" of the doctrine and concluded that the trial court "properly applied" the doctrine in dismissing the claim. *Id.*

Admittedly, both decisions state generally that "no cause of action exists for negligence" that causes only economic loss, and other language included in the opinions would appear, at first blush, to support that general notion. *Aikens*, 501 A.2d at 278-79; *Adams*, 816 A.2d at 305, 307. However, a closer examination reveals that, when read in context, the court's observations are made in reference to **employees'** attempt to bring negligence claims for damages arising out of the contract/relationship they had with their employer, of which the tortfeasor was unaware. Thus, those generalized pronouncements do not support the conclusion that all negligence claims for economic losses are barred under Pennsylvania law.

- 1 I agree with the majority's footnoted treatment of Section 302B, see Majority Opinion, at — n.11, but my present emphasis is on the interplay between contract and tort in that particular context. I also have difficulty with the majority's framing of the duty in issue presented here in terms of a broader duty of care pertaining to affirmative conduct that runs to the public at large. See *id.* at — —.
- 2 My conclusion, in this regard, is similar to that stated by the majority in Part A of its opinion, albeit that I view the present matter as entailing a special relationship arising, in the first instance, out of contractual undertakings.
- 3 Moreover, as noted above, I disagree with the majority's conclusion that a duty on the part of an employer to safeguard confidential personal and financial information provided by **employees** as a condition of their employment exists independently of a contractual employment relationship.
Parenthetically, **Employees'** complaint does not attempt to delineate the specific nature of the employment relationships involved among the 62,000 putative class members. Presumably, there are individual written contracts, collective bargaining agreements, and oral agreements involved. In all events -- and while realizing that the Court has referred to oral at-will employment relationships as "non-contractual," *Weaver v. Harpster*, 601 Pa. 488, 502, 975 A.2d 555, 563 (2009) -- I believe that a contract overlay is initially appropriate for present purposes in each of the above categories. Accord Howard C. Ellis, *Employment-at-Will and Contract Principles: The Paradigm of Pennsylvania*, 96 DICK. L. REV. 595, 613 (1992) (explaining, that under the terms of at-will employment relationships, "[e]ach day is a new contract on these terms: a day's work for a day's pay").
- 4 The gist of the action doctrine serves as a means by which courts categorize claims to maintain the distinction between theories of breach of contract and tort. See generally *Bruno v. Erie Ins. Co.*, 630 Pa. 79, 111-12, 106 A.3d 48, 68-69 (2014). Under that doctrine, I would ultimately view **Employees'** claims as properly couched in negligence, despite the hybrid character, in light of Section 302B of the Restatement.
- 5 This is not to say that certification of a class action is necessarily proper, particularly relative to damages issues. See generally *Samuel-Bassett v. Kia Motors Am., Inc.*, 613 Pa. 371, 472-77, 34 A.3d 1, 61-65 (2011) (Saylor, J., dissenting).
- 6 I also agree with the majority that the General Assembly's passage of an enactment requiring notification to affected persons of **data** breaches -- and even its consideration of potential civil causes of action in connection therewith -- does not control whether **Employees'** claims sufficiently comport with traditional common law principles to survive a demurrer. See Majority Opinion, at — n.10. In other words, in light of the preexisting norms, the failure of the Legislature to pass affirmative legislation is inadequate, in my view, to signal an abrogation of those norms.
This assessment subsumes consideration of the economic loss doctrine -- in light of all of the uncertainties attending the doctrine, it seems to me to be unreasonable to assume that the Legislature would have deemed it sufficient to effectively extinguish potential common law causes of action regarding **data** breaches.

 KeyCite Yellow Flag - Negative Treatment
Distinguished by American Tooling Center, Inc. v. Travelers Casualty
and Surety Company of America, 6th Cir.(Mich.), July 13, 2018

731 Fed.Appx. 929

This case was not selected for publication in West's
Federal Reporter.

See Fed. Rule of Appellate Procedure 32.1 generally
governing citation of judicial decisions issued on or
after Jan. 1, 2007. See also U.S. Ct. of App. 11th Cir.
Rule 36-2.

United States Court of Appeals, Eleventh Circuit.

INTERACTIVE COMMUNICATIONS
INTERNATIONAL, INC. et al.,
Plaintiff-Appellants,
v.
GREAT AMERICAN INSURANCE CO.,
Defendant-Appellee.

No. 17-11712

|
(May 10, 2018)

Synopsis

Background: Insured under crime protection policy
which provided coverage for computer fraud brought
action claiming breach of contract and bad faith and
seeking damages, declaratory relief, and statutory penalty.
Parties cross-moved for summary judgment. The United
States District Court for the Northern District of Georgia,
No. 1:15-cv-02671-WSD, 2017 WL 1021749, granted
insurer's motion. Insured appealed.

Holdings: The Court of Appeals held that:

^[1] scam involving multiple redemptions of chits loaded on
debit cards was perpetrated through "the use of a[]
computer" within meaning of policy, but

^[2] insured's loss did not "result[] directly" from the
computer fraud, as required by policy's plain language.

Affirmed.

^[1] Insurance

☞ Theft or Burglary

Fraud against insured seller of chits to
consumers the value of which was loaded on
debit cards was perpetrated through "the use of
a[] computer" within meaning of crime
protection policy; even if cardholders did not
realize that their telephone calls resulted in
interaction with a computers that processed
transaction requests, they interfaced directly
with insured's computer system to effect
duplicate redemptions of chits.

1 Cases that cite this headnote

^[2] Insurance

☞ Combined or concurrent causes

Insurance

☞ Theft or Burglary

Loss by insured operator of network that
allowed consumers to put money onto general
purpose reloadable debit cards issued by banks
from scam involving multiple redemptions of
single chits did not "result[] directly" from a
computer fraud, as required by crime protection
policy's plain language; although fraudsters'
manipulation of insured's computers set into
motion the chain of events that ultimately led to
insured's loss, that loss was temporally remote
in that days, weeks, or even months or years
could pass between fraudulent chit redemption
and the ultimate disbursement of the
fraud-tainted funds, and chain of causation
involved intervening acts and actors between
first step fraud and fourth step loss.

1 Cases that cite this headnote

Attorneys and Law Firms

*930 Kristen Kabat Bromberek, Daniel F. Diffley, Tejas

West Headnotes (2)

S. Patel, Alston & Bird, LLP, Atlanta, GA, for Plaintiff-Appellant

Michael A. Graziano, F. Joseph Nealon, Eckert Seamans Cherin & Mellott, LLC, Washington, DC, H. Michael Bagley, Drew Eckl & Farnham, LLP, Atlanta, GA, for Defendant-Appellee

Appeal from the United States District Court for the Northern District of Georgia, D.C. Docket No. 1:15-cv-02671-WSD

Before MARCUS and NEWSOM, Circuit Judges, and BUCKLEW, District Judge.

Opinion

PER CURIAM:

This insurance-coverage case arises out of a “Computer Fraud” policy issued by Great American Insurance Company to Interactive Communications International, Inc. and HI Technology Corp. (together, “InComm”). InComm sells “chits”—each of which has a specific monetary value—to consumers, who can then “redeem” them by loading their value onto a debit card. InComm lost a lot of money—\$11.4 million—when fraudsters manipulated a glitch in InComm’s computerized interactive-telephone system that enabled them to redeem chits multiple times, with each duplicative redemption of an already-redeemed chit defrauding InComm of the chit’s value. We hold, though, that InComm’s insurance policy does not cover its loss. Although the fraudsters did “use [a] computer” within the meaning of the policy, we conclude that InComm’s loss did not “result[] directly” from the computer fraud, as required by the policy’s plain language.

I

InComm operates a network that allows consumers to put money onto general-purpose reloadable debit cards issued by banks. In particular, InComm sells “chits” to consumers, which they can then use to transfer funds to their cards. After purchasing a chit at a retailer like CVS or Walgreens, a consumer can simply call InComm to redeem the chit and have its value moved over to his card.

When a consumer dials InComm’s 1-800 number to

redeem a chit, he is connected to InComm’s interactive voice response (“IVR”) computer system. The IVR system uses eight computers that process voice requests or telephone touch-tone codes. To redeem a chit through InComm’s IVR, a consumer enters his debit card number and the PIN located on the back of the chit. The IVR then credits the value of the chit to the card, and the funds become immediately available to the cardholder.

After making the funds available for use, InComm is contractually obligated to transfer money, equivalent to the value of the redeemed chit(s), to the bank that issued the debit card. By contract, InComm is obligated to transfer the funds *931 within 15 days, although as a matter of standard practice, InComm typically does so within 24 hours. The funds are maintained in the card-issuing bank, for the cardholder’s benefit, until he uses the card to conduct a transaction. Because InComm’s computer system immediately credits the value of a redeemed chit to a debit card, a cardholder could make purchases using a debit card before or after funds sufficient to cover the value of the redeemed chit are transferred from InComm to the card-issuing bank.

Between November 2013 and May 2014, fraudsters exploited a vulnerability in InComm’s IVR system that enabled multiple redemptions of a single chit. Specifically, the fraudsters figured out that they could redeem a single chit multiple times by making two or more concurrent calls to the IVR system and simultaneously requesting the redemption of a particular chit. One call would transfer the funds from the chit to the debit card account, while the other would return the chit to an “unredeemed” state, allowing it to be redeemed again. Over seven months, InComm’s system processed 25,553 fraudulent redemptions associated with 1,988 individual chits.

The fraudulent redemptions cost InComm \$11.4 million. The vast majority of that loss—\$10.7 million—was redeemed on debit cards issued by Bancorp bank. It is that \$10.7 million sum that is at issue in this case. Pursuant to InComm’s contract with Bancorp, InComm sold chits to consumers and provided the IVR computer system that allowed the users to transfer the chit’s value to their Bancorp-issued debit cards. Once InComm’s IVR system was used to redeem a chit, the chit’s value was made available for use on the Bancorp card. Bancorp was obligated to transfer funds to merchants to cover purchases made using their debit cards, and InComm, in turn, was obligated to transfer funds equivalent to the value of the redeemed chit(s) to a Bancorp account through which Bancorp pays for those purchases.

The fraudsters' simultaneous calls to InComm's IVR system resulted in duplicate funds being made immediately available on Bancorp customers' debit cards. Because InComm believed the transactions to be legitimate, it wired funds to Bancorp to cover the purchasing power made available on the cards.

II

The insurance policy at issue protects InComm against "Computer Fraud." In particular—and the language is important—the policy provides coverage for "loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person (other than a messenger) outside those premises; or (b) to a place outside those premises."

InComm seeks coverage for the \$10.7 million lost to Bancorp debit card holders who fraudulently manipulated InComm's IVR system to effectuate duplicate redemptions of InComm chits.

The district court granted Great American's motion for summary judgment. It held that the computer-fraud policy did not cover InComm's claimed loss for two reasons. First, the court concluded that the fraud was not accomplished through "the use of a[] computer" within the meaning of InComm's policy; and second, it held that, in any event, InComm's loss did not "result[] directly" from the use (computer or otherwise) of the IVR system. Although we disagree with the district court's determination that the fraudsters' simultaneous *932 phone calls to the IVR system did not constitute "use of a[] computer," we agree with the court's conclusion that InComm's loss did not "result[] directly" from the computer fraud. Accordingly, we affirm the district court's judgment that InComm's loss is not covered.

III

¹⁴Great American contends, and the district court concluded, that the policy does not cover InComm's claimed loss because the scam was not perpetrated through "the use of a[] computer." We disagree.

All parties agree that the IVR system comprises eight computers that process transaction requests from cardholders. Thus, the dispute over the "use of a[] computer" provision reduces to the question whether phone calls made to a computer system constitute "use" of that computer system.

The district court started with the dictionary definitions of the terms "computer" and "telephone." Based on those definitions, it concluded that "[a] 'telephone' is not a 'computer' " but, rather, "a completely different device." Thus, the court held, the phones with which fraudsters had dialed the IVR system were not computers within the meaning of InComm's policy.

But because the fraud here involved both telephones and computers, we cannot stop there. The question is whether the fraudsters "use[d]" both phones and computers to perpetrate their scheme—namely, *using* the phones to manipulate—and thereby *use*—the IVR computers. In rejecting InComm's argument, the district court seems to have imposed additional conditions not required by the policy's plain language—for instance, that the computer "use" be knowing. *See, e.g.*, Dist. Ct. Op. at 26 ("There is no record evidence that cardholders even realized their telephone calls resulted in interaction with a computer.").

But the plain meaning of the word "use"—indeed, as evidenced in the very definitions cited by the district court—comfortably supports an understanding that encompasses the callers' access and manipulation of InComm's IVR system. The district court, for instance, cited both the Oxford Dictionaries' online definition of the term "use" to mean "take, hold, or deploy (something) as a means of accomplishing or achieving something; employ," and *Webster's Encyclopedic Unabridged Dictionary's* definition to mean "to employ for some purpose; put into service; make use of." *Oxford Dictionaries*, <https://en.oxforddictionaries.com/definition/use>; *Webster's Encyclopedic Unabridged Dictionary of the English Language* 2097 (2001). Those definitions, it seems to us, fit like a glove. Here, the callers clearly "deploy[ed]"—or "employ[ed]"—the IVR computer system "as a means of accomplishing or achieving" fraudulent duplicate redemptions of InComm chits. *See Oxford Dictionaries*, <https://en.oxforddictionaries.com/definition/use>. So too, under the district court's Webster's-based definition, the callers "used" the IVR system, "employ[ing]" it "for some purpose; put[ting it] into service; mak[ing] use of" it. *See Webster's Encyclopedic Unabridged Dictionary of the English Language* (2001).

Other dictionaries confirm what the district court's own indicate. *Webster's Second New International Dictionary*, for instance, defines "use" as "to convert to one's service; to avail oneself of; to employ." *Webster's New International Dictionary* at 2806 (2d ed. 1939). There simply can be no doubt that the fraudsters "convert[ed]" InComm's IVR computer system to their service and "avail[ed]" themselves of it by submitting fraudulent reload requests *933 to the computer system in a way that yielded duplicate chit redemptions. To be clear, it is not the case, as the district court suggested, that the IVR system was just "somehow involved" in the fraudsters' scheme, or that the system was merely "engaged at any point in the causal chain." Rather, the fraudsters interfaced directly with the IVR computer system to effectuate their duplicate redemptions. Thus, we conclude that the fraud against InComm was perpetrated through the "use of a[] computer" within the terms of its insurance policy.

IV

¹²But that is not the end. The question remains whether the "loss of ... money" that InComm suffered here "result[ed] directly" from the use of the IVR. Like the district court, we conclude that it did not.¹ In explaining why, we must explore two sub-issues. First, as a matter of law, what exactly does the phrase "result[] directly" mean? And second, as a matter of fact, when did InComm's loss occur?

A

Not surprisingly, the parties have different views about what it means for a loss to "result[] directly" from a computer fraud. For its part, InComm contends—not without some support—that the policy's "resulting directly" language entails only a showing of proximate cause. See, e.g., *Scirex Corp. v. Fed. Ins. Co.*, 313 F.3d 841, 850 (3d Cir. 2002) (applying Pennsylvania law that equates "direct cause" with "proximate cause"); see also *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F.3d 821, 831-32 (6th Cir. 2012) (holding that under Ohio law, a "proximate cause" standard should be used "to determine whether plaintiffs

sustained loss 'resulting directly from' the 'theft of Insured property by Computer Fraud' "). With its own cases in tow, Great American urges us instead to adopt a reading of "resulting directly" that requires immediacy between conduct and result. See, e.g., *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed.Appx. 252, 258 (5th Cir. 2016) (declining to extend coverage where a loss caused by a fraudulent transfer was "the result of other events and not directly [caused] by the computer use").²

Rather than following the thread of close-but-not-quite-on-point cases from other jurisdictions, however, we look to the plain language of InComm's policy. It is a fundamental principle of Georgia law—and law more generally—that words in contracts "generally bear their usual and common signification[.]" Ga. Code Ann. § 13-2-2(2); accord, e.g., A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* at 69 (2012) ("The ordinary meaning rule is the most fundamental semantic rule of interpretation. It governs constitutions, statutes, rules, and private instruments."). Accordingly, if the phrase "resulting directly" has a "common signification"—i.e., an ordinary meaning—then we have to find and enforce it.

The dispute here, of course, is not about the term "resulting," but rather the word "directly": What does it mean for a result to follow a cause "directly"? Common-language and legal dictionaries provide a clear (and essentially the same) answer. *Webster's Second*, for instance, defines "direct" to mean "(1) straight; proceeding from one point to another in time or space without deviation or interruption; not crooked or oblique ...; (2) Straightforward; going straight to the point ...; (3) Immediate; marked by the absence of an intervening agency or influence; making contact or effected without an intermediary[.]" *Webster's New International Dictionary* at 738 (2d ed. 1939). In the same way, *Black's* defines "direct" to mean "(1) straight, undeviating; (2) straightforward; (3) free from extraneous influence, immediate; (4) of, relating to, or involving passing in a straight line of descent, as distinguished from a collateral line." *Black's Law Dictionary* at 265 (10th ed. 2014).

The theme is unmistakable. In accordance with the term's ordinary meaning, we hold that, for purposes of InComm's policy, one thing results "directly" from another if it follows straightaway, immediately, and without any intervention or interruption.

B

Which leads to the factual question: When, exactly, did InComm's loss occur? And based on the answer to that question, did InComm's loss "result[] directly" (as we have interpreted that phrase) from the fraudsters' misuse of InComm's IVR computer system?

We conclude that although the fraudsters' manipulation of InComm's computers set into motion the chain of events that ultimately led to InComm's loss, their use of the computers did not "directly"—which is to say immediately and without intervention or interruption—cause that loss. To the contrary, several steps typically intervened between the fraudulent manipulation of the IVR system to enable duplicate chit redemptions, on the front end, and InComm's ultimate loss, on the back. Here is a timeline of sorts:

- **Step 1:** The fraudsters manipulate InComm's IVR system to enable a duplicate chit redemption. For each fraudulently redeemed chit, a fraudster's debit card is immediately credited with purchasing power, but InComm's funds are neither transferred, nor disturbed, nor altered in any way.
- **Step 2:** Shortly after processing a redemption call through the IVR system, InComm transfers money (equal to the amount of the redeemed chits) to an account at Bancorp for the purpose of paying debts incurred by debit card holders. Bancorp maintains the account "for the benefit of" InComm as "holder[] of the Cardholder Balances for the benefit of [Debit] Cardholders." Although InComm is contractually obligated to transfer funds to the Bancorp account within 15 days of making the corresponding purchasing power available on debit cards, as a matter of regular business practice it transfers the money to Bancorp within 24 hours. The funds remain in the Bancorp account until needed to cover purchases made on a consumer's debit card.
- **Step 3:** A debit card user makes a purchase from a merchant, incurring *935 debt to be paid from the InComm-earmarked Bancorp account.
- **Step 4:** Bancorp transfers money from the account to the merchant to cover the purchase made by the cardholder.³

InComm insists that its loss occurred at Step 2—and is thus "directly" the result of the Step-1 fraud. In particular, InComm says that upon transfer of funds to the account held by Bancorp, it lost both ownership and control of those funds. But the facts of the case demonstrate otherwise—that, in fact, InComm retained at least some

control over the funds held by Bancorp even after the Step-2 transfer, and could prevent their loss by intervening to halt the disbursement of money from the Bancorp account to merchants at Step 4. On one particular occasion, after identifying fraud associated with \$1.9 million in duplicate redemptions by some debit card holders, InComm stepped in to prevent the cards from engaging in further transactions. InComm did so unilaterally, and indeed did not even inform Bancorp that it had done so for nearly a month. That \$1.9 million was not "los[t]"; rather, it remains to this day in the InComm-earmarked account held by Bancorp.

Accordingly, InComm's loss did not occur with the Step-2 transfer of funds to the account held by Bancorp. Rather, the loss did not occur until—at Step 4—Bancorp actually disbursed money from the InComm-earmarked account to pay merchants for purchases made by cardholders. That was the point at which InComm could not recover its money. That was the point of no return.

That being the case, it seems clear to us that InComm's loss did not "result[] directly" from the initial computer fraud. Far from being immediate, the loss was temporally remote: days or weeks—even months or years—could pass between the fraudulent chit redemption and the ultimate disbursement of the fraud-tainted funds from InComm's Bancorp account. And it is not just that the loss was remote in time; the chain of causation involved intervening acts and actors between the Step-1 fraud and the Step-4 loss. Even after a chit was fraudulently redeemed, each of the following had to occur: (1) InComm had to transfer money to the Bancorp account; (2) the cardholder had to make a purchase using fraudulently obtained funds; and (3) Bancorp had to disburse money from InComm's account to cover the purchase and pay the merchant. It was only at that point that InComm's loss truly materialized. The lack of immediacy—and the presence of intermediate steps, acts, and actors—makes clear that the loss did not "result[] directly" from the initial fraud.

V

Because InComm's loss did not "result[] directly" from the fraudulent use of its *936 IVR computer system, the loss is not covered by its insurance policy. We therefore affirm the district court's grant of summary judgment in favor of Great American.

AFFIRMED.

731 Fed.Appx. 929

All Citations

Footnotes

* Honorable Susan C. Bucklew, United States District Judge for the Middle District of Florida, sitting by designation.

1 We assume for the purposes of this opinion—without deciding—that the use of the IVR "fraudulently cause[d] a transfer of ... property from inside the ... banking premises ... to a person [or] place outside those premises" within the meaning of InComm's policy.

2 The delta between the parties' competing readings may be smaller than it appears. As Justice Cardozo taught us years ago, proximate cause serves to limit liability, not expand it. See *Palsgraf v. Long Island R. Co.*, 248 N.Y. 339, 162 N.E. 99, 101 (1928). To that end, *Black's* defines "Proximate Cause," in relevant part, as "[a] cause that *directly* produces an event and without which the event would not have occurred.—Also termed (in both senses) *direct* cause; *direct* and proximate cause...." *Black's Law Dictionary* at 265 (10th ed. 2014) (emphasis added). *Webster's Second* provides a similar definition: "[A] cause which *directly* or with no mediate agency produces an effect; specifically in law, that which in ordinary natural sequence produces a specific result, no independent disturbing agencies intervening." *Webster's New International Dictionary* at 1995 (2d ed. 1939).

3 In the ordinary course, the fraud and transfer of funds would proceed as sequenced here. It is at least possible, however, that the expenditure of the fraudulently obtained funds could occur almost immediately after the commission of the fraud. Therefore, even though InComm transfers funds to Bancorp within 24 hours of a chit redemption, it is possible that a cardholder might spend fraudulently obtained funds before InComm makes the corresponding transfer to Bancorp. Despite this potential variation in the sequencing of steps leading to InComm's loss, InComm has always maintained that its loss occurred at the moment it transferred funds to Bancorp, not at the moment that fraudulently obtained purchasing power was used by cardholders. See, e.g., Br. of Appellant 21 ("InComm's loss ... occurred when the money was transferred to Bancorp."). Thus, the potential for variation in the timing of cardholder purchases in the fraud-loss sequence does not change the outcome of this case. We are not obliged to consider arguments not raised by the parties. See *United States v. Campa*, 529 F.3d 980, 989 (11th Cir. 2008) (arguments not made in a party's initial brief are abandoned).

268 F.Supp.3d 471
United States District Court, S.D. New York.

MEDIDATA SOLUTIONS, INC., Plaintiff,
v.
FEDERAL INSURANCE CO., Defendant

15-CV-907 (ALC)

Signed 07/21/2017

Synopsis

Background: Insured corporation, which wired millions of dollars to unknown actor as a result of e-mail “spoofing” scheme, brought action against insurer, challenging insurer’s denial of insured’s claim under policy covering losses caused by certain criminal and fraudulent acts. Parties filed cross-motions for summary judgment.

Holdings: The District Court, Andrew L. Carter, Jr., J., held that:

^[1] insured’s losses were covered under computer fraud clause;

^[2] insured’s losses were covered under funds transfer fraud clause; and

^[3] insured’s losses were not covered by forgery clause.

Insured’s motion granted; insurer’s motion denied.

West Headnotes (8)

- ^[1] **Insurance**
⇒ Application of rules of contract construction

Under New York law, insurance policies are interpreted according to general rules of contract interpretation.

Cases that cite this headnote

- ^[2] **Contracts**
⇒ Intention of Parties

Under New York law, the fundamental, neutral precept of contract interpretation is that agreements are construed in accord with the parties’ intent.

Cases that cite this headnote

- ^[3] **Contracts**
⇒ Language of Instrument

Under New York law, a written agreement that is complete, clear and unambiguous on its face must be enforced according to the plain meaning of its terms.

Cases that cite this headnote

- ^[4] **Contracts**
⇒ Ambiguity in general

Under New York law, when a contract is unambiguous, its interpretation is a question of law.

Cases that cite this headnote

- ^[5] **Insurance**
⇒ Reasonable expectations
Insurance
⇒ Plain, ordinary or popular sense of language

In determining whether an insurance contract is ambiguous, a court applying New York law should focus on the reasonable expectations of the average insured upon reading the policy and

employing common speech.

Cases that cite this headnote

[6]

Insurance

☛ Theft or Burglary

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were covered under computer fraud clause in crime protection policy; scheme amounted to deceitful and dishonest access of insured's computer system, as the fraud was achieved by entry into insured's e-mail system with spoofed e-mails that used computer code to mask the thief's true identity, and while insured's employees took other steps before approving the wire transfer, the transfer was still the direct result of the spoofed e-mails.

2 Cases that cite this headnote

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were not covered under forgery clause in crime protection policy; even if the spoofed e-mails constituted a forgery, the policy only covered forgeries or alterations of a financial instrument.

Cases that cite this headnote

Attorneys and Law Firms

*472 Adam Seth Ziffer, Robin L. Cohen, Alexander Michael Sugzda, McKool Smith, New York, NY, for Plaintiff

Christopher M. Kahler, Sara Gronkiewicz-Doran, Scott Schmookler, Gordon & Rees LLP, Chicago, IL, Jeffrey Yehuda Aria Spiegel, Joseph Salvo, Gordon & Rees, LLP, New York, NY, for Defendant

[7]

Insurance

☛ Theft or Burglary

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were covered under funds transfer fraud clause in crime protection policy; given that the wire transfer depended on obtaining the consent of several high level employees by trick, the fact that insured's accounts payable employee willingly sent the transfer did not transform it into a valid transaction.

Cases that cite this headnote

**MEMORANDUM AND ORDER GRANTING
SUMMARY JUDGMENT**

ANDREW L. CARTER, JR., District Judge:

Medidata Solutions, Inc. ("Medidata") commenced this action against Federal Insurance Company ("Federal") after Federal denied Medidata's claim for insurance coverage. The parties filed cross-motions for summary judgment and the Court ordered additional expert discovery. For the following reasons, Medidata's motion for summary judgment is GRANTED.

[8]

Insurance

☛ Theft or Burglary

BACKGROUND

A. Medidata

Medidata provides cloud-based services to scientists conducting research in clinical trials. Medidata's Memorandum of Law in Support of Motion for Summary Judgment ("Pl's Mem.") at 3, ECF No. 37. Medidata used Google's Gmail platform for company emails. Affidavit of Glenn Watt in Support of Medidata's Motion for Summary Judgment, ("Watt Aff.") ¶ 2, ECF No. 39. Medidata email addresses consisted of an employee's first initial and last name followed by the domain name "mdsol.com" instead of "gmail.com". *Id.* ¶ 3. Email messages sent to Medidata employees were routed through Google computer servers. *Id.* ¶ 4. Google systems processed and stored the email messages. *Id.* ¶ 4. During processing, Google compared an incoming email address with Medidata employee profiles in order to find a match. *Id.* ¶ 9. If a match was found, Gmail displayed the sender's full name, email address, and picture in the "From" field of the message. *Id.* ¶¶ 8, 10, 11. After processing, the emails were displayed in the Medidata employee's email account. *Id.* ¶ 7. Medidata employees used computers owned by the company to *473 access the email messages that were process and displayed by Google. *Id.*

B. Fraud on Medidata

In the summer of 2014, Medidata notified its finance department of the company's short-term business plans which included a possible acquisition. Plaintiff's Rule 56.1 Statement ("Pl.'s 56.1") ¶ 36, ECF No. 36. Medidata instructed finance personnel "to be prepared to assist with significant transactions on an urgent basis." *Id.* ¶ 37. In 2014, Alicia Evans ("Evans") worked in accounts payable at Medidata. *Id.* ¶ 38. Evans was responsible for processing all of Medidata's travel and entertainment expenses. Joint Exhibit Stipulation ("Joint Ex. Stip.") Ex. 20, 41:16–21, ECF No. 41. On September 16, 2014, Evans received an email purportedly sent from Medidata's president. *Id.* Ex. 2. The email message contained the president's name, email address, and picture in the "From" field. *Id.* The message to Evans stated that Medidata was close to finalizing an acquisition, and that an attorney named Michael Meyer ("Meyer") would contact Evans. *Id.* The email advised Evans that the acquisition was strictly confidential and instructed Evans to devote her full attention to Meyer's demands. *Id.* Evans replied: "I will certainly assist in any way I can and will make this a priority." *Id.* Ex. 4.

On that same day, Evans received a phone call from a man who held himself out to be Meyer. *Id.* Ex. 20, 31:10–15. Meyer demanded that Evans process a wire transfer for him. *Id.* Meyer told Evans a physical check would not suffice because of time constraints. *Id.* Ex. 20, 36:5–8. Evans explained to Meyer that she needed an email from Medidata's president requesting the wire transfer. *Id.* Ex. 20, 34:17–20. Evans also explained she needed approval from Medidata Vice President Ho Chin ("Chin"), and Director of Revenue Josh Schwartz ("Schwartz"). *Id.*

Chin, Evans, and Schwartz then received a group email purportedly sent from Medidata's president stating: "I'm currently undergoing a financial operation in which I need you to process and approve a payment on my behalf. I already spoke with Alicia, she will file the wire and I would need you two to sign off." *Id.* Ex. 6. The email contained the president of Medidata's email address in the "From" field and a picture next to his name. *Id.* In response, Evans logged on to Chase Bank's online system to initiate a wire transfer. *Id.* Ex. 20, 13:20–14:16. Evans entered the banking information provided by Meyer and submitted the wire transfer for approval. *Id.* Ex. 20, 15:11–23, 16:17–17:05. Schwartz and Chin logged on to Chase's online banking system and approved the wire transfer. *Id.* Ex. 21, 13:20–14:16; Ex. 19, 59:16–18, 60:02–04. \$4,770,226.00 was wired to a bank account that was provided by Meyer. *Id.* Ex. 8.

On September 18, 2014, Meyer contacted Evans requesting a second wire transfer. *Id.* Ex. 20, 42:02–10. Evans initiated the second wire transfer and Schwartz approved it. *Id.* Ex. 21, 40:24–41:20. However, Chin thought the email address in the "Reply To" field seemed suspicious. *Id.* Ex. 19, 46:08–24. Chin spoke with Evans about his suspicions and Evans composed a new email to Medidata's president inquiring about the wire transfers. *Id.* Ex. 20, 50:04–20. Medidata's president told Evans and Chin that he had not requested the wire transfers. *Id.* Medidata employees then realized that the company had been defrauded. *Id.* Ex. 19, 63:09–64:18. Medidata contacted the FBI and hired outside counsel to conduct an investigation. *Id.* The investigations revealed that an unknown actor altered the emails that were sent to Chin, Evans, and Schwartz to appear *474 as if they were sent from Medidata's president. *Id.*

C. Medidata Insurance Policy

Medidata held a \$5,000,000 insurance policy with Federal

called “Federal Executive Protection”. *Id.* Ex. 1. The Policy contained a “Crime Coverage Section” addressing loss caused by various criminal acts, including Forgery Coverage Insuring, Computer Fraud Coverage, and Funds Transfer Fraud Coverage. *Id.*

issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization’s knowledge or consent.” *Id.*

1. Computer Fraud Coverage

The Policy’s, “Computer Fraud Coverage”, protected the “direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party.” *Id.* The Policy defined “Organization” as “any organization designated in Item 4 of the Declarations for this coverage section.” *Id.* Item 4, in turn, lists “Medidat[a] Solutions, Inc., and its subsidiaries” as a covered Organization. *Id.* The Policy defined “Third Party” as “a natural person other than: (a) an Employee; or (b) a natural person acting in collusion with an Employee.” *Id.*

The Policy defined “Computer Fraud” as: “[T]he unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation.” *Id.* A “Computer Violation” included both “the fraudulent: (a) entry of Data into ... a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format ... directed against an Organization.” *Id.* The Policy defined “Data” broadly to include any “representation of information.” *Id.* The Policy defined “Computer System” as “a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned and operated by an Organization; (b) leased and operated by an Organization; or (c) utilized by an Organization.” *Id.*

2. Funds Transfer Fraud Coverage

The Policy’s Funds Transfer Fraud Coverage protected “direct loss of Money or Securities sustained by an Organization resulting from Funds Transfer Fraud committed by a Third Party.” *Id.* The Policy defined “Funds Transfer Fraud” as: “fraudulent electronic ... instructions ... purportedly issued by an Organization, and

3. Forgery Coverage

The Policy’s Forgery Coverage protected “direct loss sustained by an Organization resulting from Forgery or alteration of a Financial Instrument committed by a Third Party”. *Id.* “Forgery” is defined as “the signing of the name of another natural person ... with the intent to deceive ... Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures.” *Id.*

4. Claim For Coverage

On September 25, 2014, Medidata submitted a claim to Federal requesting coverage of the fraud under three clauses. *Id.* Ex. 11. Federal assigned regional claims technician Michael Maillet (“Maillet”) to investigate the fraud on Medidata. *Id.* Ex. 12.

On December 24, 2014, Federal denied Medidata’s claim for coverage. *Id.* Federal denied coverage under the computer fraud clause, because there had been no “fraudulent entry of Data into Medidata’s computer system.” *Id.* at 4. As support, Federal *475 explained that [t]he subject emails containing false information were sent to an inbox which was open to receive emails from any member of the public” thus the entry of the fictitious emails “was authorized.” *Id.* In addition, Federal concluded that there had been no “change to data elements” because the emails did not cause any fraudulent change to data elements or program logic of Medidata’s computer system. *Id.* Federal conceded that Gmail added the name and picture of Medidata’s president because of the email, however, Federal stated that the fake email did not cause this to happen. *Id.* According to Federal, Medidata’s computer system, “populated the email in the normal manner.” *Id.* at 5.

Federal denied coverage under the funds transfer fraud clause because the wire transfer had been authorized by

Medidata employees and thus was made with the knowledge and consent of Medidata. *Id.*

Finally, Federal rejected Medidata's claim for Forgery Coverage because the emails did not contain an actual signature and did not meet the Policy's definition of a Financial Instrument. *Id.* Federal also based its denial of both the Forgery Coverage and the Computer Fraud Coverage claims on the belief that the emails did not directly cause Medidata's loss, because no loss would have taken place if Medidata employees had not acted on the instructions contained in those emails. *Id.*

On January 13, 2015, Medidata sent a letter responding to the denial and setting forth the basis for coverage under the Policy. *Id.* Ex. 14. Federal replied on January 30, 2015, reasserting its denial of coverage for the claim. *Id.* Ex. 15.

DISCUSSION

Summary judgment is appropriate where "the pleadings, depositions, answers to interrogatories and admissions on file, together with affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986); *see also* Fed. R. Civ. P. 56(c). "There is no issue of material fact where the facts are irrelevant to the disposition of the matter." *Chartis Seguros Mexico, S.A. de C.V. v. HLI Rail & Rigging, LLC*, 967 F.Supp.2d 756, 761 (S.D.N.Y. 2013). "Speculation, conclusory allegations and mere denials are not enough to raise genuine issues of fact." *Id.* (citing *National Union Fire Ins. Co. of Pittsburgh, Pa. v. Walton Ins. Ltd.*, 696 F.Supp. 897, 900 (S.D.N.Y. 1988)).

The burden lies with the moving party to demonstrate the absence of any genuine issue of material fact and all inferences and ambiguities are to be resolved in favor of the nonmoving party. *See Celotex Corp.*, 477 U.S. at 323, 106 S.Ct. 2548 (1986); *see also Hotel Emps. & Rest. Emps. Union, Local 100 v. City of New York Dep't of Parks & Recreation*, 311 F.3d 534, 543 (2d Cir. 2002). If "no rational jury could find in favor, of the nonmoving party because the evidence to support its case is so slight, there is no genuine issue of material fact and a grant of summary judgment is proper." *Gallo v. Prudential Residential Servs., Ltd. P'ship*, 22 F.3d 1219, 1224 (2d Cir. 1994). An identical standard applies where the parties

file cross-motions for summary judgment: "each party's motion must be examined on its own merits, and in each case all reasonable inferences must be drawn against the party whose motion is under consideration." *Morales v. Quintel Entm't, Inc.*, 249 F.3d 115, 121 (2d Cir. 2001) (citation omitted).

[1] [2] [3] [4] [5] Under New York law, insurance policies are interpreted according to general rules of contract interpretation. *476 *Olin Corp. v. Am. Home Assur. Co.*, 704 F.3d 89, 98 (2d Cir. 2012). "The fundamental, neutral precept of contract interpretation is that agreements are construed in accord with the parties' intent. ... [A] written agreement that is complete, clear and unambiguous on its face must be enforced according to the plain meaning of its terms." *Bank of New York v. First Millennium, Inc.*, 598 F.Supp.2d 550, 556 (S.D.N.Y. 2009) *aff'd*, 607 F.3d 905 (2d Cir. 2010) (citing *Greenfield v. Philles Records, Inc.*, 98 N.Y.2d 562, 569, 750 N.Y.S.2d 565, 780 N.E.2d 166 (2002)). When a contract is unambiguous, its interpretation is a question of law. *See 82-11 Queens Blvd. Realty, Corp. v. Sunoco, Inc. (R & M)*, 951 F.Supp.2d 376, 381 (E.D.N.Y. 2013). In determining whether an insurance contract is ambiguous, a Court should focus "on the reasonable expectations of the average insured upon reading the policy and employing common speech." *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.*, 25 N.Y.3d 675, 680, 16 N.Y.S.3d 21, 37 N.E.3d 78 (2015).

A. Computer Fraud Coverage

[6] Medidata argues that the Policy's Computer Fraud clause covers the company's loss in 2014, because a thief fraudulently entered and changed data in Medidata's computer system. Pl.'s Mem. at 14–20. Specifically, Medidata asserts that the address in the "From" field of the spoofed emails constituted data which was entered by the thief posing as Medidata's president. *Id.* at 14. Also, a thief entered a computer code which caused Gmail to "change" the hacker's email address to the Medidata president's email address. *Id.* at 19–20.

Federal argues that Medidata's loss in 2014 is not covered by the Computer Fraud clause, because the emails did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information. Federal's Memorandum of Law in Support of Summary Judgment ("Def's Mem.") at 9–12, ECF No. 34. The Court has reviewed the Policy and concludes that, as a matter of law, the unambiguous language of the Computer Fraud clause provides coverage for the theft

from Medidata.

Under Medidata's policy, a computer violation occurs upon the "the fraudulent: (a) entry of Data into or deletion of Data from a Computer System" or "(b) change to Data elements or program logic of a Computer System, which is kept in machine readable format." The New York Court of Appeals shed light on these phrases in *Universal*, which involved a health insurance company that was defrauded by healthcare providers who entered claims for reimbursement of services that were never rendered. 25 N.Y.3d at 681–82, 16 N.Y.S.3d 21, 37 N.E.3d 78.¹ *Universal* sought insurance coverage for the losses incurred by the fraudulent claims. *Id.* at 679, 16 N.Y.S.3d 21, 37 N.E.3d 78. *Universal*'s computer fraud clause covered "loss resulting directly from a fraudulent entry of Electronic Data or Computer Program into, or change of Electronic Data or Computer Program within" the insured's computer system." *477 *Id.* In denying coverage, the Court of Appeals held that the unambiguous language of *Universal*'s policy "applie[d] to losses incurred from unauthorized access to *Universal*'s computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users." *Id.* at 680–81, 16 N.Y.S.3d 21, 37 N.E.3d 78. The court reasoned that the drafter's "intentional placement of 'fraudulent' before 'entry' and 'change' manifest[ed] the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access." *Id.* at 681, 16 N.Y.S.3d 21, 37 N.E.3d 78.

Here, the fraud on Medidata falls within the kind of "deceitful and dishonest access" imagined by the New York Court of Appeals. *Id.* It is undisputed that the theft occurred by way of email spoofing.² Joint Factual Stipulation Following Discovery ("Joint Fact Stip.") ¶ 7, ECF 72. To that end, the thief constructed messages in Internet Message Format ("IMF") which the parties compare to a physical letter containing a return address. *Id.* ¶ 2. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ("SMTP"). *Id.* ¶ 1. Much like a physical envelope, the SMTP Envelope contained a recipient and a return address. *Id.* To mask the true origin of the spoofed emails, the thief embedded a computer code. *Id.* ¶ 10. The computer code caused the SMTP Envelope and the IMF Letter to display different email addresses in the "From" field. *Id.* The spoofed emails showed the thief's true email address in the SMTP "From" field, and Medidata's president's email address in the IMF "From" field. *Id.* ¶¶ 20–21. When Gmail received the spoof emails, the system compared the address in the IMF "From" field with a list of contacts and populated Medidata's president's name

and picture. *Id.* ¶ 15. The recipients of the Gmail messages only saw the information in the IMF "From" field. *Id.* ¶ 11.

Federal's reading of *Universal* is overbroad. In this case, Federal focuses on the thief's construction of the spoofed emails and computer code before sending them to Gmail, arguing that, as a result, there was no entry or change of data to Medidata's computer system. Def's Mem. at 9–12. Under this logic, *Universal* would require that a thief hack into a company's computer system and execute a bank transfer on their own in order to trigger insurance coverage. However, this reading of *Universal* incorrectly limits the coverage of the policy in this case. It is true that the Court of Appeals in *Universal* peppered its opinion with references to hacking as the example for a covered violation. See e.g., *id.* at 681, 16 N.Y.S.3d 21, 37 N.E.3d 78 ("[T]he rider covers losses from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be 'hacking' of the computer system."). But a hacking is one of many methods a thief can use, and "is an everyday term for unauthorized access to a computer system." *Dial Corp. v. News Corp.*, No. 13-CV-6802, 2016 WL 690868, at *3 (S.D.N.Y. Feb. 17, 2016) (citation omitted). Thus, *Universal* is more appropriately read as finding coverage for fraud where the perpetrator violates the *478 integrity of a computer system through unauthorized access and denying coverage for fraud caused by the submission of fraudulent data by authorized users. *Id.* (noting "[o]ther language in the rider confirms that the rider seeks to address unauthorized access"). Indeed, an examination of the trial court's analysis in *Universal* further emphasizes this point. The N.Y. Supreme Court held *Universal*'s policy "indicates that coverage is for an unauthorized entry into the system, i.e. by an unauthorized user, such as a hacker, or for unauthorized data, e.g. a computer virus." The trial court was also concerned with unauthorized users and corrupting data instead of authorized users submitting untruthful content.³ *Id.* ("Nothing in this clause indicates that coverage was intended where an authorized user utilized the system as intended, i.e. to submit claims, but not where the claims themselves were fraudulent.").

Federal's reliance on *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, is also misplaced. The court in *Pestmaster*, held that a corporation's computer fraud insurance policy did not cover a theft by the company's payroll administrator, because the administrator was authorized to withdraw funds from the corporation's bank account, notwithstanding the fact that he later misappropriated the payroll funds. No. 13-CV-5039 (JFW), 2014 WL 3844627, at *6 (C.D. Cal. July 17, 2014). Relying on *Universal*, the Court explained that

“Computer Fraud occurs when someone hacks or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds.” *Id.* (internal quotation marks omitted). In contrast, the fraud on Medidata was achieved by entry into Medidata’s email system with spoofed emails armed with a computer code that masked the thief’s true identity. The thief’s computer code also changed data from the true email address to Medidata’s president’s address to achieve the email spoof.

In challenging causation, Federal contends that “there is no direct nexus” between the spoofed emails and the fraudulent wire transfer. Defs Mem. at 13–15. According to Federal, the spoofed emails “did not create, authorize, or release a wire transfer” because Medidata employees received telephone calls from the thief and took other steps in approving the fraudulent transfer. *Id.* at 16. As support, Federal cites to the Fifth Circuit’s decision in *Apache Corp. v. Great American Ins. Co.* denying coverage of a similarly worded computer fraud provision. 662 Fed.Appx. 252 (5th Cir. 2016). The underlying fraud in *Apache* was achieved through a muddy chain of events. The insured was duped into sending payments to thieves that were intended for the insured’s vendor. *Id.* at 253. The thieves engaged in a concerted effort to achieve the fraud which included phone calls, spoofed emails, and falsified documents. *Id.* Applying Texas law, the Fifth Circuit held that the insured’s computer fraud provision did not cover the theft because “the fraudulent transfer was the result of other events and not directly by the computer use.” *Id.* The Court explained that the insured “invited the computer-use at issue ... even though the computer-use was but one step in Apache’s multi-step, but flawed, process that ended in its making required and authorized, *479 very large invoice payments, but to a fraudulent bank account.” *Id.* at 258–59. In contrast, Medidata employees did not invite the spoofed emails at issue. The chain of events began with an accounts payable employee receiving a spoofed email from a person posing as Medidata’s president. To the extent that the facts of this case fit within *Apache*, the Court finds its causation analysis unpersuasive. The Court finds that Medidata employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata’s president.

Federal also cites to the Ninth Circuit’s decision in *Taylor & Lieberman v. Federal Ins. Co.*, denying coverage of a computer fraud provision. (“*Taylor I*”), 681 Fed.Appx. 627, 628 (9th Cir. 2017). In *Taylor*, an accounting firm fell victim to an email spoofing scam after a thief invaded the email account of the accounting firm’s client. *Id.* at 628. The thief, disguised as the client, sent emails

requesting wire transfers to a specified bank account. *Id.* The district court keenly pointed out the “series of far more remote circumstances” than simply a theft directly from the accounting firm. *Taylor & Lieberman v. Fed. Ins. Co.*, No. 14-CV-3608 (RSWL) (SHX), 2015 WL 3824130, at *4 (C.D. Cal. June 18, 2015) (“*Taylor II*”). The district court emphasized that the thief stole money from the client not the accounting firm, and that the accounting firm was seeking reimbursement for the loss of its client’s money. *Id.* at *4. Importantly, the court added, “if the funds had been held in an account owned or attributed to Plaintiff, such as an escrow account and a hacker had entered into Plaintiff’s computer system ... then Plaintiff would be correct in asserting coverage from the Policy.” *Id.* The Ninth Circuit agreed, noting that the mere sending of emails from the client to the accounting firm did not constitute unauthorized entry into the accounting firm’s computer system. *Taylor I*, 681 Fed.Appx. at 629–30. But Medidata did not suffer a loss from spoofed emails sent from one of its clients. A thief sent spoofed emails armed with a computer code into the email system that Medidata used. Also, the fraud caused transfers out of Medidata’s own bank account. Therefore, Medidata was “correct in asserting coverage from the Policy.” *Taylor II*, 2015 WL 3824130, at *4.

Accordingly, Medidata has demonstrated that its losses were a direct cause of a computer violation.

B. Funds Transfer Fraud Coverage

^[7]Medidata argues that it was improperly denied coverage under the Funds Transfer Fraud clause because the theft in 2014 “(1) caused a direct loss of money; (2) by fraudulent electronic instructions purportedly issued by Medidata; (3) issued to a financial institution; (4) to deliver money from Medidata’s accounts; (5) without Medidata’s knowledge or consent.” Pl’s Mem. at 20. Federal challenges the last of the requisite elements, arguing that the bank wire transfer in 2014 was voluntary and with Medidata’s knowledge and consent. Def’s Mem. at 21–24. Federal also argues that, because Medidata employees voluntarily transferred the money, it was actually issued by Medidata instead of “purportedly issued” as the Policy demands. *Id.* at 24–25. The Court finds that the unambiguous language of the Policy covers the theft from Medidata in 2014.

The Policy defines Funds Transfer Fraud as: “fraudulent electronic ... instructions ... purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver

Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent." *480 Joint Ex. Stip., Ex. 1. Under *Pestmaster*, which Federal relies, a funds transfer fraud agreement, "does not cover authorized or valid electronic transactions ...even though they are, or maybe, associated with a fraudulent scheme." 2014 WL 3844627, at *5. However, *Pestmaster* involved a corporation that made several valid electronic transfers to its payroll administrator who later misappropriated the funds. *Id.* at *6. The court justified the denial of coverage by pointing out, "there is no evidence that... any third party, gained unauthorized entry into Pestmaster's bank's electronic fund transfer system or pretended to be an authorized representative or otherwise altered the electronic instructions in order to wrongfully divert money from the rightful recipient." *Id.* (emphasis added). Also unpersuasive is Federal's reliance on *Cumberland Packing Corp. v. Chubb Ins. Corp.*, which interpreted a funds transfer fraud agreement. 29 Misc.3d 1208(A), 2010 WL 3991185, at *5 (Sup. Ct. 2010). The court in *Cumberland* denied coverage to a policyholder who had voluntarily transferred funds to Bernie Madoff for investment purposes. *Id.* The court reasoned that "Madoff was expressly authorized to act as plaintiffs' broker/agent" which did not involve unauthorized instructions to transfer money. *Id.* In this case, it is undisputed that a third party masked themselves as an authorized representative, and directed Medidata's accounts payable employee to initiate the electronic bank transfer. It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties' manipulation of the emails. The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees' knowledge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny. Therefore, Medidata has demonstrated that the Funds Transfer Fraud clause covers the theft in 2014.

C. Forgery Coverage

^[8]The theft from Medidata in 2014 does not trigger coverage under the Forgery clause, because the Policy

Footnotes

¹ The trial court noted "the perpetrators enrolled new members in the ... plan with the person's cooperation, in return for which the member received a kickback from the provider. In some cases, the provider used the member's personal

requires a "direct loss resulting from Forgery or alteration of a Financial Instrument committed by a Third Party." Joint Ex. Stip., Ex. 1. The parties vehemently dispute whether the spoofed emails containing Medidata's president's name constitute a forgery. *See* Pl's Mem. at 18; Def's Mem. at 17. However, the Court need not resolve the matter. Even if the emails contained a forgery, the absence of a financial instrument proves fatal to Medidata's claim for coverage. In a strained reading of the Policy, Medidata argues that a forgery itself triggers coverage even in the absence of a financial instrument. Medidata's Memorandum of law in Further Support of Summary Judgment ("Pl's Reply") at 20, ECF No. 52. However, "[t]he entire contract must be reviewed and particular words should be considered, not as if isolated from the context, but in the light of the obligation as a whole and the intention of the parties as manifested thereby. Form should not prevail over substance and a sensible meaning of words should be sought." *Riverside S. Planning Corp. v. CRP/Extell Riverside, L.P.*, 13 N.Y.3d 398, 404, 892 N.Y.S.2d 303, 920 N.E.2d 359 (2009) (citations, alterations, and internal quotation marks omitted). Medidata's interpretation of the Policy would render the word forgery vague and create ambiguity in the clause. To the contrary, a forgery or alteration are both means by which a person can corrupt a financial instrument resulting in a loss to *481 the insured. If forgery is viewed in isolation, the Policy would certainly be converted to a general crime policy. Therefore, Medidata has not demonstrated that it suffered a loss that was covered by the Forgery clause.

CONCLUSION

For the foregoing reasons, Medidata's motion for summary judgment is **GRANTED** and Federal's motion for summary judgment is **DENIED**.

SO ORDERED.

All Citations

268 F.Supp.3d 471

information without that person's knowledge. In either event, the provider itself did not enroll in the plan. Instead, they were able to submit claims after obtaining a National Provider Identifier (NPI) from [the agency of the U.S. Department of Health and Human Service tasked with overseeing this market]. In some cases, the NPI was obtained for a fictitious provider, in other cases it was fraudulently taken from a legitimate provider."

- 2 A court in this district defined "Spoofing" as "the practice of disguising a commercial e-mail to make the e-mail appear to come from an address from which it actually did not originate. Spoofing involves placing in the "From" or "Reply-to" lines, or in other portions of e-mail messages, an e-mail address other than the actual sender's address, without the consent or authorization of the user of the e-mail address whose address is spoofed." *Karvaly v. eBay, Inc.*, 245 F.R.D. 71, 91 n.34 (E.D.N.Y. 2007) (citation and internal quotation marks omitted).
- 3 The Appellate Division appeared to have a similar concern when it found that the language of the policy "was intended to apply to wrongful acts in manipulation of the computer system, i.e., by hackers, and did not provide coverage for fraudulent content consisting of claims by bona fide doctors and other health care providers authorized to use the system for reimbursement for health care services that were not provided."

End of Document

© 2019 Thomson Reuters. No claim to original U.S. Government Works.

2018 WL 4941760 (Ill.Cir.Ct.) (Trial Pleading)
Circuit Court of Illinois.
County Department/Law Division
Cook County

MONDELEZ INTERNATIONAL, INC., Plaintiff,
v.
ZURICH AMERICAN INSURANCE COMPANY, Defendant.

No. 2018L011008.
October 10, 2018.

Jury Demanded

Complaint

John H. Mathias, Jr., David M. Kroeger, Jenner & Block, LLP (05003), 353 N. Clark Street, Chicago, Illinois 60654, (312) 222-9350.

Jan A. Larson (pro hac vice application to be submitted), Jenner & Block LLP (05003), 1099 New York Avenue, NW, Suite 900, Washington, DC 20001, (202) 639-6000.

JURY DEMAND

The undersigned demands a jury trial.

<<signature>>

(Signature)

☐ Atty. No.: 05003

Name: *JENNER & BLOCK LLP*

Atty. for: *Plaintiff, Mondelez International, Inc.*

Address: *c/o David M. Kroeger, 353 N. Clark St.*

City/State/Zip: *Chicago, Illinois 60654*

Telephone: *312.923.2861*

Primary Email: *dkroeger@jenner.com*

Secondary Email: *jmathias@jenner.com*

Tertiary Email: _____

Dated: *October 10, 2018*

Mondelez International, Inc. ("MDLZ"), through its counsel, complains as follows against Zurich American Insurance Company ("Zurich"):

1. In this insurance coverage action, MDLZ seeks relief for Zurich's breaches of its contractual obligations to MDLZ under an all-risk property insurance policy, Zurich's failure to honor promises that induced MDLZ to act to its detriment, and Zurich's bad faith conduct.

Jurisdiction and Venue

2. This Court has personal jurisdiction over Zurich pursuant to 735 ILCS 5/2-209(a)(4), in that Zurich "contract[ed] to insure any person, property or risk located within this State at the time of contracting."

3. Venue is proper in this Circuit pursuant to 735 ILCS 5/2-101, in that a substantial part of the transactions giving rise to the claim occurred here.

The Parties

4. MDLZ is one of the world's largest snack companies. MDLZ manufactures and markets snack food and beverage products for consumers in approximately 165 countries around the world. Its portfolio includes many iconic snack brands: Nabisco, Oreo, LU and belVita biscuits; Cadbury, Milka, Cadbury Dairy Milk and Toblerone chocolate; Trident gum; Halls candy and Tang powdered beverages.

5. Zurich is an insurance company organized under the laws of New York, with its headquarters in Schaumburg, Illinois. Zurich is part of the Zurich Insurance Group.

Factual Background

6. Zurich sold Property Insurance Policy No. PPR 5834380-04 (the "Policy") to MDLZ. (The Policy is voluminous, and Zurich is already in possession of a copy, so a copy is being maintained at the offices of counsel for MDLZ and will be made available to the Court and Zurich upon request.)

7. The Policy provides annual coverage incepting November 1, 2016, for "all risks of physical loss or damage" to MDLZ's property, specifically including "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction"

8. The Policy also specifically provided other types of coverage, including but not limited to "TIME ELEMENT" coverage, including for "Actual Loss Sustained and EXTRA EXPENSE incurred by the Insured during the period of interruption directly resulting from the failure of the Insured's electronic data processing equipment or media to operate" resulting from malicious cyber damage.

9. On June 27, 2017, MDLZ fell victim to two separate malicious introductions of "malware" machine code or instruction, which later came to be referred to by some sources as "NotPetya," into two of its servers at different physical locations and at different times. The two malware introductions/occurrences spread from these two servers, stole credentials of numerous users, propagated across the MDLZ network, and rendered permanently dysfunctional approximately 1700 of MDLZ's servers and 24,000 of its laptops.

10. As a result of the damage caused both to its hardware and operational software systems, MDLZ incurred property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins, and other covered losses aggregating well in excess of \$100,000,000.

11. MDLZ gave prompt notice to Zurich and thereafter worked with Zurich personnel to adjust the insurance claim. As part of this effort, MDLZ provided Zurich with (i) voluminous amounts of information, including information quantifying and substantiating the extent of MDLZ's losses; and (ii) access to MDLZ employees as well as consultants retained by MDLZ to provide explanations pertinent to its claim.

12. During this time, Zurich publicly and, on information and belief, in its non-public dealings with actual and prospective policyholders who were considering the purchase or renewal of insurance coverage from Zurich, portrayed the NotPetya malware as a form of "ransomware" that merited the continued (if not increased) purchase of insurance coverage from Zurich. For example, on March 5, 2018, Alison Martin, Group Chief Risk Officer for the Zurich Insurance Group, published an article containing the following statement:

"Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses of USD 300 million for a number of affected businesses."

13. Nevertheless, by letter dated June 1, 2018, Zurich informed MDLZ that it was denying coverage under the Policy based on a single Policy exclusion, Exclusion B.2(a), which provides:

B. This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:

...

2) a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:

(i) government or sovereign power (de jure or de facto);

(ii) military, naval, or air force; or

(iii) agent or authority of any party specified in i or ii above.

Zurich asserted no other exclusion and stated no other ground for denying coverage under the Policy in its June 1, 2018 denial letter.

14. As an insurer seeking to deny insurance coverage on the basis of an exclusion, Zurich bears the burden of proving the applicability of the single exclusion (Exclusion B.2(a)) on which it based its June 1, 2018 denial of coverage.

15. Zurich's invocation of a "hostile or warlike action" exclusion to deny coverage for malicious "cyber" incidents was, on information and belief, unprecedented. Indeed, and also on information and belief, the purported application of this

type of exclusion to anything other than conventional armed conflict or hostilities was unprecedented. Accordingly, on this basis alone, Zurich wrongfully denied coverage to MDLZ.

16. Furthermore, the loss and damage for which MDLZ claims coverage under the Policy did not result from a cause or event excluded under Exclusion B.2(a) of the Policy. The two incursions of malicious code or instruction into MDLZ's computers did not constitute "hostile or warlike action," as required by Exclusion B.2(a). Nor was the loss and damage for which MDLZ claims coverage under the Policy directly or indirectly caused by "hostile or warlike action." In the alternative, Exclusion B.2(a) is vague and ambiguous, particularly given Zurich's failure to modify that historical language to specifically address the extent to which it would apply to cyber incidents, and therefore must be interpreted in favor of coverage.

17. On information and belief, Zurich senior management itself recognized that the June 1, 2018 coverage denial was wrongful and improper, and further recognized the potential for MDLZ to initiate immediate litigation that would publicize Zurich's ill-advised coverage denial in a manner that would adversely impact its dealings with actual and prospective policyholders who were considering the purchase or renewal of insurance coverage from Zurich.

18. Accordingly, to induce MDLZ not to initiate immediate coverage litigation, and in what now appears to be an improper effort to allow Zurich to try to avoid publicity for and/or "mend" its June 1, 2018 coverage denial, Zurich promised MDLZ that it would rescind its June 1, 2018 declination of coverage and resume adjustment of MDLZ's insurance claim. These promises were intended to convince MDLZ to refrain from filing immediate litigation.

19. On July 18, 2018, Zurich sent an email to MDLZ that "formally rescind[ed]" its coverage denial and promised to resume the adjustment of MDLZ's insurance claim. On July 24, 2018, Zurich sent an email to MDLZ committing to advance a \$10,000,000 partial payment toward MDLZ's insurance claim. Zurich initially sought to place conditions on the advance, but after pushback from MDLZ a few days later Zurich's Head of Property Claims sent an email representing to MDLZ that the promised advance would be unconditional and "not subject to a 'claw back' provision."

20. In reliance upon Zurich's representations concerning (i) the rescission of its denial of coverage based upon Exclusion B.2(a); and (ii) the resumption of its adjustment of MDLZ's insurance claim, including the advance of an unconditional \$10,000,000 partial payment, MDLZ refrained to its detriment from instituting immediate litigation challenging the June 1, 2018 denial letter. MDLZ instead agreed to meet with Zurich representatives regarding adjustment and payment of its insurance claim. MDLZ would not have done so were it not for these explicit representations and promises from Zurich.

21. However, despite "formally rescind[ing]" its coverage denial and promising to resume the adjustment of MDLZ's insurance claim (including advancement of an unconditional \$10,000,000 partial payment), Zurich has in all material respects continued to behave as if it were still asserting the applicability of Exclusion B.2(a) to deny coverage entirely to MDLZ. In particular, Zurich: (i) refused to advance an unconditional partial payment of \$10,000,000 on MDLZ's insurance claim; (ii) refused to make any other claim payment whatsoever; and (iii) otherwise failed to resume and finalize the adjustment of MDLZ's claim.

22. By at least October 2018, MDLZ's patience had run out, and Zurich knew that. With knowledge that MDLZ was planning to file this lawsuit if Zurich did not take steps to immediately resolve its insurance claim, Zurich on October 9, 2018 sent MDLZ a letter purporting to "reassert" its June 1, 2018 declination of coverage based on Exclusion B.2(a). Zurich's "reassertion" did not cite any new material facts or developments occurring since Zurich's unequivocal "rescission" of its denial of coverage on July 18, 2018. Zurich's October 9 letter also belatedly sought to raise new coverage defenses in an improper effort to "mend" its June 1, 2018 declination of coverage, which had consciously omitted any other possible grounds for denying coverage, thereby waiving them. Zurich was aware of all of these purported additional coverage defenses as of June 1, 2018, but elected not to include them in its coverage denial letter of that date. Under the circumstances, Zurich's attempted October 9, 2018 "reassertion" of its denial of coverage is null, void and without effect.

COUNT I

Breach of Contract

(Wrongful Refusal to Pay Insurance Claim)

23. MDLZ restates and incorporates paragraphs 1 through 22 above as if fully set forth herein.

24. MDLZ provided and Zurich received timely notice of MDLZ's insured losses.

25. Zurich investigated and/or had the opportunity to investigate MDLZ's claim for more than 11 months, and to fairly explore whatever bases it may have believed it had for denying or limiting coverage. Zurich based its June 1, 2018 declination of coverage on a single ground: Exclusion B.2(a). Its denial letter asserted no other basis for the denial of coverage.

26. Zurich's June 1, 2018 denial of coverage was wrongful and constituted a breach of its obligations under the Policy.

27. Zurich's purported "reassertion" of its denial of coverage on October 9, 2018, was also wrongful and constituted a breach of its obligations under the Policy.

28. As a direct and proximate result of Zurich's breaches of contract, MDLZ has been deprived of the benefits of the insurance coverage sold by Zurich, and has incurred at least \$100,000,000 in damages as a result, subject to any applicable deductibles.

COUNT II

Breach of Contract

(Wrongful Refusal to Withdraw Coverage Denial and Pay Insurance Claim)

29. MDLZ restates and incorporates paragraphs 1 through 22 above as if fully set forth herein.

30. In exchange for MDLZ refraining from the immediate filing of litigation that would have challenged the June 1, 2018 coverage denial and publicized Zurich's wrongful interpretation of Exclusion B.2(a) to the insurance marketplace, and in particular actual and prospective policyholders, Zurich made contractual commitments to MDLZ (i) to rescind its June 1, 2018 declination of coverage; and (ii) resume adjustment of MDLZ's insurance claim, including the immediate advancement of an unconditional partial payment of \$10,000,000 to MDLZ.

31. Zurich has refused to honor these commitments, and has instead continued to behave in all material respects as if it were still denying coverage to MDLZ based on Exclusion B.2(a). Zurich has refused to make any payment whatsoever on MDLZ's insurance claim, including the unconditional partial payment of \$10,000,000 it had committed in writing to advance.

32. As a direct and proximate result of Zurich's breaches of contract, MDLZ has been deprived of the benefits of the contractual promises made by Zurich and accepted by MDLZ, and has incurred damages as a result.

COUNT III

Promissory Estoppel

33. MDLZ restates and incorporates paragraphs 1 through 22 above as if fully set forth herein.

34. Zurich unambiguously promised MDLZ that it was (i) rescinding its June 1, 2018 declination of coverage; and (ii) resuming adjustment of MDLZ's insurance claim, including the immediate advance of an unconditional partial payment of \$10,000,000 to MDLZ. Zurich did so for the purpose of, inter alia, inducing MDLZ not to file immediate litigation challenging its June 1, 2018 denial of coverage.

35. MDLZ relied on Zurich's promises by refraining from the filing of immediate litigation that would have, inter alia, publicized Zurich's wrongful interpretation of Exclusion B.2(a) to the insurance marketplace, and in particular actual and prospective policyholders of Zurich.

36. MDLZ's reliance was expected and foreseeable by Zurich.

37. MDLZ relied to its detriment on Zurich's promises, none of which have been fulfilled, and has been damaged as a result.

38. Having induced MDLZ to rely to its detriment upon explicit promises, Zurich should be held to those promises and should be, inter alia, estopped both from (i) reasserting Exclusion B.2(a) as a basis for denying coverage; and (ii) asserting any other additional ground for denying coverage which could have been asserted on June 1, 2018.

COUNT IV

Vexatious and Unreasonable Conduct

Illinois Insurance Code Section 155

39. MDLZ restates and incorporates paragraphs 1 through 38 above as if fully set forth herein.

40. Zurich has acted vexatiously and unreasonably by, among other things, the following, all in violation of 215 ILCS 5/155:

a. improperly denying MDLZ's insurance claim on June 1, 2018;

b. refusing to honor its explicit promises to MDLZ to (i) rescind its June 1, 2018 declination of coverage; and (ii) resume adjustment of MDLZ's insurance claim, including the immediate advancement of an unconditional partial payment of \$10,000,000 to MDLZ; and

c. Improperly "reasserting" its denial of coverage on October 9, 2018.

41. MDLZ has been damaged by Zurich's vexatious and unreasonable conduct, in that it has effectively been denied the benefits of the insurance coverage for which it contracted and for which MDLZ collected a premium. MDLZ has also been improperly forced to incur the burden, expense and further disruption of bringing and pursuing this action.

Prayer for Relief

WHEREFORE, MDLZ respectfully requests that the Court grant it the following:

1. An award of the damages that MDLZ has sustained, in the amount of at least \$100,000,000, subject to any applicable deductibles, and such other amounts to be determined at trial;
2. An order enforcing Zurich's promises to MDLZ to (i) rescind its June 1, 2018 declination of coverage; and (ii) resume adjustment of MDLZ's insurance claim, including the immediate advancement of an unconditional partial payment of \$10,000,000 to MDLZ, including barring Zurich from both (i) reasserting Exclusion B.2(a) as a basis for denying coverage; and (ii) asserting any other additional ground for denying coverage which could have been asserted on June 1, 2018; and further declaring null, void and without effect Zurich's attempted October 9, 2018 "reassertion" of its denial of coverage;
3. An award of pre-judgment and post-judgment interest on MDLZ's damages, in the full amount permitted by law;
4. An award of the costs, including attorneys' fees, that MDLZ incurs in connection with bringing and pursuing this action, along with the maximum statutory penalty that 215 ILCS 5/155 allows; and
5. Such additional relief in MDLZ's favor as the Court deems appropriate.

Jury Demand

MDLZ demands a trial by jury on all issues triable to a jury.

MONDELEZ INTERNATIONAL, INC.

By: <<signature>>

One of Its Attorneys

Dated: October 10, 2018

John H. Mathias, Jr.

David M. Kroeger

JENNER & BLOCK, LLP (05003)

353 N. Clark Street

Chicago, Illinois 60654

(312) 222-9350

Jan A. Larson (*pro hac vice application to be submitted*)

JENNER & BLOCK LLP (05003)

1099 New York Avenue, NW

Suite 900

Washington, DC 20001

(202) 639-6000

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.

2016 WL 3055111

Only the Westlaw citation is currently available.
United States District Court,
D. Arizona.

P.F. Chang's China Bistro, Inc., Plaintiff,
v.
Federal Insurance Company, Defendant.

No. CV-15-01322-PHX-SMM

|
Signed 05/26/2016

|
Filed 05/31/2016

ORDER

Honorable Stephen M. McNamee, Senior United States District Judge

*1 Pending before the Court is Defendant Federal Insurance Company's ("Federal") Motion for Summary Judgment. (Doc. 22.) P.F. Chang's China Bistro, Inc. ("Chang's") has responded and the matter is fully briefed. (Docs. 36, 38.) The Court heard Oral Arguments on the motion on April 19, 2016. (Doc. 41.) In essence, the main issue before the Court is whether coverage exists under the insurance policy between Chang's and Federal for the credit card association assessments that arose from the data breach Chang's suffered in 2013. The Court now issues following ruling.

I. FACTUAL BACKGROUND¹

¹ The facts are undisputed unless indicated otherwise.

A. The CyberSecurity Insurance Policy

Federal sold a CyberSecurity by Chubb Policy ("Policy") to Chang's corporate parent, Wok Holdco LLC, with effective dates from January 1, 2014 to January 1, 2015. (Doc. 8-1 at 2.) On its website, Federal marketed the Policy as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world" that "[c]overs direct loss, legal liability, and consequential loss resulting from cyber security breaches." (Doc. 37-7.) Specific provisions of the Policy will be defined and discussed in greater detail below.

During the underwriting processes, Federal classified Chang's as a high risk, "PCI Level 1", client because Chang's conducts more than 6 million transactions per year. (Docs. 37-1 at 121-22, 37-6.) Further, because of the large number of Chang's transactions conducted with customer credit cards, Federal noted there was high exposure to potential customer identity theft. (Doc. 37-6.) In 2014, Chang's paid an annual premium of \$134,052.00 for the Policy. (Doc. 37-1 at 126.)

B. The Master Service Agreement Between Chang's and BAMS

Chang's and other similarly situated merchants are unable to process credit card transactions themselves. Merchants must enter into agreements with third-party "Servicers" or "Acquirers" who facilitate the processing of credit card transactions with the banks who issue the credit cards ("Issuers"), such as Chase or Wells Fargo. Here, Chang's entered into a Master Service Agreement ("MSA") with Bank of America Merchant Services ("BAMS") to process credit card payments made by Chang's customers. (Doc. 23-2.) Under the MSA, Chang's delivers its customers' credit card payment information to BAMS who then settles the transaction through an automated clearinghouse; BAMS then credits Chang's account for the amount of the payment. (*Id.*)

Servicers like BAMS perform their processing obligations pursuant to agreements with the credit card associations ("Associations"), like MasterCard and Visa. (Doc. 24-1.) BAMS' agreement with MasterCard is governed by the MasterCard Rules, and are incorporated in its MSA with Chang's. (*See Id.*; Doc. 23-2.) Under the MasterCard Rules, BAMS is obligated to pay certain fees and assessments ("Assessments") to MasterCard in the event of a data breach or "Account Data Compromise" ("ADC"). (Doc. 24-1 at § 10.2) These Assessments include "Operational Reimbursement" fees and "Fraud Recovery" fees, and they are calculated by formulae set forth in the MasterCard Rules. (*Id.*)

*2 Under the MSA, Chang's agreed to compensate or reimburse BAMS for "fees," "fines," "penalties," or "assessments" imposed on BAMS by the Associations. (*See* Doc. 23-2 at 9, 18.) Section 13.5 of the Addendum to the MSA reads: "[Chang's] agrees to pay [BAMS] any fines, fees, or penalties imposed on [BAMS] by any Associations, resulting from Chargebacks and any other fines, fees or penalties imposed by an Association with respect to acts or omissions of [Chang's]." (*Id.* at 9.) Section 5 of Schedule A

to the Addendum to the MSA provides: "In addition to the interchange rates, [BAMS] may pass through to [Chang's] any fees assessed to [BAMS] by the [Associations], including but not limited to, new fees, fines, penalties and assessments imposed by the [Associations]." (*Id.* at 18.)

C. The Security Compromise

On June 10, 2014, Chang's learned that computer hackers had obtained and posted on the Internet approximately 60,000 credit card numbers belonging to its customers (the "security compromise" or "data breach"). (Doc. 25-1.) Chang's notified Federal of the data breach that very same day. (*Id.*)

To date, Federal has reimbursed Chang's more than \$1,700,000 pursuant to the Policy for costs incurred as a result of the security compromise. (Doc. 22 at 9.) Those costs include conducting a forensic investigation into the data breach and the costs of defending litigation filed by customers whose credit card information was stolen, as well as litigation filed by one bank that issued card information that was stolen. (*Id.*)

Following the data breach, on March 2, 2015, MasterCard issued an "ADC Operational Reimbursement/Fraud Recovery Final Acquirer Financial Responsibility Report" to BAMS. (Doc. 26-2.) This MasterCard Report imposed three Assessments on BAMS, a Fraud Recovery Assessment of \$1,716,798.85, an Operational Reimbursement Assessment of \$163,122.72 for Chang's data breach, and a Case Management Fee of \$50,000. (*Id.*; Doc. 26-3.) The Fraud Recovery Assessment reflects costs, as calculated by MasterCard, associated with fraudulent charges that may have arisen from, or may be related to, the security compromise. (Doc. 1-1 at ¶20.) The Operational Reimbursement Assessment reflects costs to notify cardholders affected by the security compromise and to reissue and deliver payment cards, new account numbers, and security codes to those cardholders. (*Id.* at ¶19) The Case Management Fee is a flat fee and relates to considerations regarding Chang's compliance with Payment Card Industry Data Security Standards. (*Id.* at ¶18.)

D. The BAMS Letter

On March 11, 2015, BAMS sent Chang's a letter (the "BAMS Letter") stating:

MasterCard's investigation concerning the account data compromise event involving [Chang's] is now complete.

[BAMS] has been notified by MasterCard that a case management fee and Account Data Compromise (ADC) Operational Reimbursement and Fraud Recovery (ORFR) are being assessed against [BAMS] as a result of the data compromise. In accordance with your [MSA] you are obligated to reimburse [BAMS] for the following assessments:

- \$ 50,000.00 – Case Management Fee
- \$ 163,122.72 – ADC Operational Reimbursement
- \$1,716,798.85 – ADC Fraud Recovery

\$1,929,921.57²

(Doc. 26-3.) Chang's notified Federal of the BAMS Letter on March 19, 2015 and sought coverage for the Assessments. (Doc. 26-4.) Pursuant to the MSA, and in order to continue operations and not lose its ability to process credit card transactions, Chang's reimbursed BAMS for the Assessments on April 15, 2015. (Doc. 1-1 at ¶24.) Federal denied coverage for the Assessments and Chang's subsequently filed this lawsuit.

- 2 This total is separate from and does not include the \$1.7 million Federal has already paid Chang's under the Policy.

II. STANDARD OF REVIEW

"The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed.R.Civ.P. 56(a). "The substantive law determines which facts are material; only disputes over facts that might affect the outcome of the suit under the governing law properly preclude the entry of summary judgment." *Nat'l Ass'n of Optometrists & Opticians v. Harris*, 682 F.3d 1144, 1147 (9th Cir. 2012) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). To prove the absence of a genuine dispute, the moving party must demonstrate that "the evidence is such that [no] reasonable jury could return a verdict for the nonmoving party." *Liberty Lobby*, 477 U.S. at 248. In determining whether a party has met its burden, a court views the evidence in the light most favorable to the non-moving party and draws all reasonable inferences in the non-moving party's favor. *Liberty Lobby*, 477 U.S. at 255. While a court may consider only admissible evidence in ruling on a motion for summary judgment, the focus is not "on the admissibility of the evidence's form," but "on the admissibility of its

contents.” Fraser v. Goodale, 342 F.3d 1032, 1036–37 (9th Cir. 2003).

*3 Federal courts sitting in diversity apply the forum state's choice of law rules to determine controlling substantive law. Klaxon Co. v. Stentor Elec. Mfg. Co. Inc., 313 U.S. 487, 496 (1941). Arizona adheres to Restatement (Second) of Conflict of Laws § 193 (1971), which states that insurance contracts are generally governed “by the local law of the state which the parties understood was to be the principal location of the insured risk during the term of the policy.” Beckler v. State Farm Mut. Auto. Ins. Co., 195 Ariz. 282, 286, 987 P.2d 768, 772 (App. 1999). Since the principal location of the insured was in Arizona and the insurance agreement was entered into in Arizona, Arizona law governs the enforcement of the Policy.

“The traditional view of the law of contracts is that a written agreement adopted by the parties will be viewed as an integrated contract which binds those parties to the terms expressed within the four corners of the agreement.” Darner Motor Sales, Inc. v. Universal Underwriters Ins. Co., 140 Ariz. 383, 390, 682 P.2d 388, 395 (1984). However, “the usual insurance policy is a special kind of contract,” *id.*, in part because it is not “arrived at by negotiation between the parties,” Zuckerman v. Transamerica Ins. Co., 133 Ariz. 139, 144, 650 P.2d 441, 446 (1982). Instead, “[i]t is largely adhesive; some terms are bargained for, but most terms consist of boilerplate, not bargained for, neither read nor understood by the buyer, and often not even fully understood by the selling agent.” Darner, 140 Ariz. at 391, 682 P.2d at 396. Moreover, “[t]he adhesive terms generally are self-protective; their major purpose and effect often is to ensure that the drafting party will prevail if a dispute goes to court.” Gordinier v. Aetna Cas. & Sur. Co., 154 Ariz. 266, 271, 742 P.2d 277, 282 (1987). Accordingly, “special contract rules should apply.” *Id.*

Interpretation of insurance policies is a question of law. Sparks v. Republic Nat. Life Ins. Co., 132 Ariz. 529, 534, 647 P.2d 1127, 1132 (1982). “Provisions of insurance policies are to be construed in a manner according to their plain and ordinary meaning,” *id.*, but if a clause is reasonably susceptible to different interpretations given the facts of the case, the clause is to be construed “by examining the language of the clause, public policy considerations, and the purpose of the transaction as a whole,” State Farm Mut. Auto. Ins. Co. v. Wilson, 162 Ariz. 251, 257, 782 P.2d 727, 733 (1989). “[T]he general rule is that while coverage clauses are interpreted

broadly so as to afford maximum coverage to the insured, exclusionary clauses are interpreted narrowly against the insurer.” Scottsdale Ins. Co. v. Van Nguyen, 158 Ariz. 476, 479, 763 P.2d 540, 543 (App. 1988).

Furthermore, “the policy may not be interpreted so as to defeat the reasonable expectations of the insured.” Samsel v. Allstate Ins. Co., 204 Ariz. 1, 4, 59 P.3d 281, 284 (2002). “Under this doctrine, a contract term is not enforced if one party has reason to believe that the other would not have assented to the contract if it had known of that term.” First Am. Title Ins. Co. v. Action Acquisitions, LLC, 218 Ariz. 394, 400, 187 P.3d 1107, 1113 (2008); accord Averett v. Farmers Ins. Co., 177 Ariz. 531, 533, 869 P.2d 505, 507 (1994) (quoting Gordinier, 154 Ariz. at 272, 742 P.2d at 283); Darner, 140 Ariz. at 392, 682 P.2d at 397. “One of the basic principles which underlies [the doctrine] is simply that the language in the portion of the instrument that the customer is not ordinarily expected to read or understand ought not to be allowed to contradict the bargain made by the parties.” Averett, 177 Ariz. at 533, 869 P.2d at 507 (quoting State Farm Mut. Auto. Ins. Co. v. Bogart, 149 Ariz. 145, 151, 717 P.2d 449, 455 (1986), superseded by statute on other grounds as recognized in Consolidated Enters., Inc. v. Schwindt, 172 Ariz. 35, 38, 833 P.2d 706, 709 (1992)).

*4 The insured bears the burden of proving the applicability of the reasonable expectations doctrine at trial. State Farm Fire & Cas. In. Co. v. Grabowski, 214 Ariz. 188, 190, 150 P.3d 275, 277 (App. 2007). The doctrine applies only if two predicate conditions are present. First, the insured's “expectation of coverage must be objectively reasonable.” Millar v. State Farm Fire and Cas. Co., 167 Ariz. 93, 97, 804 P.2d 822, 826 (App. 1990). Second, the insurer “must have had a reason to believe that the [insured] would not have purchased the... policy if they had known that it included” the complained of provision. Grabowski, 214 Ariz. at 193–94, 150 P.3d at 280–81. Provided both of these conditions are satisfied, “Arizona courts will not enforce even unambiguous boilerplate terms in standardized insurance contracts in a limited variety of situations.” Gordinier, 154 Ariz. at 272, 742 P.2d at 283.

Finally, insurers expressly obligate themselves to defend their insureds against any claim of liability potentially covered by the policy. Ariz. Prop. & Cas. Ins. Guar. Fund v. Helme, 153 Ariz. 129, 137, 735 P.2d 451, 459 (1987); United Servs. Auto. Ass'n v. Morris, 154 Ariz. 113, 118, 741 P.2d 246, 250 (1987). The duty to defend is triggered if the

complaint “alleges facts which come within the coverage of the liability policy..., but if the alleged facts fail to bring the case within the policy coverage, the insurer is free of such obligation.” Kepner v. Western Fire Ins. Co., 109 Ariz. 329, 331, 509 P.2d 222, 224 (1973) (quoting C.T. Drechsler, Annotation, Allegations in Third Person's Action Against Insured as Determining Liability Insurer's Duty to Defend, 50 A.L.R.2d 458 § 3, at 464 (1956)). Indeed, an insurer rightfully refuses to defend only if the facts, including those outside the complaint, indisputably foreclose the possibility of coverage. See Kepner, 109 Ariz. at 331, 509 P.2d at 224. “If the insurer refuses to defend and awaits the determination of its obligation in a subsequent proceeding, it acts at its peril, and if it guesses wrong it must bear the consequences of its breach of contract.” Id. at 332, 509 P.2d at 225.

III. ANALYSIS

In its Complaint, Chang's alleges that the Policy's Insuring Clauses cover each assessment from the BAMS Letter. Specifically, Chang's claims that Insuring Clause A covers ADC Fraud Recovery Assessment, Insuring Clause B covers the ADC Operational Reimbursement Assessment, and Insuring Clause D.2 covers the Case Management Fee. (Doc. 1-1.) Federal summarily argues that the BAMS Letter and the Assessments set forth therein do not fall within the coverage provided by any of the Policy's Insuring Clauses. (Doc. 22 at 7.) Additionally, Federal contends that certain exclusions contained in the Policy bar coverage. (Id. at 11-16) The Court will analyze each Policy provision and exclusion in turn. Then the Court will turn to Chang's final argument that coverage is proper under the reasonable expectation doctrine.

A. Insuring Clause A.

Insuring Clause A provides that, “[Federal] shall pay for Loss³ on behalf of an Insured on account of any Claim first made against such Insured... for Injury.” (Doc. 8-1.) In relevant part, Claim means “a written request for monetary damages...against an Insured for an Injury.” (Id.) Under the Policy, Injury is a broad term encompassing many types of injuries, including Privacy Injury. (Id.) Privacy Injury “means injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record, or exceeding access to such Person's Record.” (Id.) Person is a natural person or an organization. (Id.) Relevant to this discussion, Record includes “any information concerning a natural person that is defined as: (i) private personal information; (ii) personally identifiable information...pursuant to any federal,

state...statute or regulation,...where such information is held by an Insured Organization or on the Insured Organization's behalf by a Third Party Service Provider” or “an organization's non-public information that is...in an Insured's or Third Party Service Provider's care, custody, or control.” (Id.) “Third Party Service Provider means an entity that performs the following services for, or on behalf of, an Insured Organization pursuant to a written agreement: (A) processing, holding or storing information; (B) providing data backup, data storage or data processing services.” (Id.)

3 Terms in bold are defined in the Policy.

*5 Federal argues that Insuring Clause A is inapplicable because BAMS, itself, did not sustain a Privacy Injury because it was not its Records that were compromised during the data breach. (Doc. 22 at 8.) Federal therefore contends that BAMS is not even in a position to assert a valid Privacy Injury Claim.

Conversely, Chang's argues that it was the Issuers who suffered a Privacy Injury because it was their Records, constituting private accounts and financial information, which were compromised in the data breach. (Doc. 36 at 6.) Chang's argument is premised upon the idea that it is immaterial that this Injury first passed through BAMS before BAMS in turn charged Chang's, because this was done pursuant to industry standards and Chang's payment to BAMS was functionally equivalent to compensating the Issuers.⁴ (See Id.) Basically, Chang's argues that because a Privacy Injury exists and was levied against it, regardless of who suffered it, the Injury is covered under the Policy. (Id.)

4 Chang's bolsters this argument by analogizing it to subrogation in other insurance contexts, which Federal misinterprets as the crux of Chang's argument. In reaching its decision, the Court gave appropriate weight to Chang's analogy, but does not believe this matter is governed by any subrogation legal rules.

Although the Court is expected to broadly interpret coverage clauses so as to provide maximum coverage for an insured, a plain reading of the policy leads the Court to the conclusion that Insuring Clause A does not provide coverage for the ADC Fraud Recovery Assessment. Scottsdale Ins. Co., 158 Ariz. at 479, 763 P.2d at 543. The Court agrees with Federal; BAMS did not sustain a Privacy Injury itself, and therefore cannot maintain a valid Claim for Injury against Chang's. The definition of Privacy Injury requires an “actual or potential unauthorized access to such Person's Record, or

exceeding access to *such Person's Record*.” (Doc. 8-1) (emphasis added). The usage of the word “such” means that only the **Person** whose **Record** is actually or potentially accessed without authorization suffers a **Privacy Injury**. Here, because the customers' information that was the subject of the data breach was not part of BAMS' **Record**, but rather the **Record** of the issuing banks, BAMS did not sustain a **Privacy Injury**.⁵ Thus, BAMS did not make a valid **Claim** of the type covered under Insuring Clause A against Chang's.

⁵ BAMS also did not sustain any other type of **Injury** as defined under the Policy.

Contrary to Chang's assertion, this interpretation is not a “pixel-level view” that “reduce[s] coverage to a mere sliver of what the plain language provides.” (Doc. 36 at 9.) Rather, this is the only result that can be derived from the Policy. It is also worth noting that Federal is not outright denying coverage in its entirety. Federal has reimbursed Chang's nearly \$1.7 million for valid claims brought by injured customers and Issuers. As will be addressed more fully below, if Chang's, who is a sophisticated party, wanted coverage for this Assessment, it could have bargained for that coverage. However, as is, coverage does not exist under the Policy for the ADC Fraud Recovery Assessment under Insuring Clause A.

B. Insuring Clause B.

Insuring Clause B provides that “[Federal] shall pay **Privacy Notification Expenses** incurred by an **Insured** resulting from [**Privacy**] **Injury**.” (Doc. 8-1.) The Policy defines **Privacy Notification Expenses** as “the reasonable and necessary cost[s] of notifying those **Persons** who may be directly affected by the potential or actual unauthorized access of a **Record**, and changing such **Person's** account numbers, other identification numbers and security codes...” (Id.) Chang's alleges that the ADC Operational Reimbursement fee is a **Privacy Notification Expense** because it compensates Issuers for the cost of reissuing bankcards and new account numbers and security codes to Chang's customers. (Docs. 1-1, 36 at 8.)

*6 In its motion, Federal uses similar argumentation it employed for Insuring Clause A. Federal contends that The ADC Operational Recovery fee was not personally incurred by Chang's, but rather was incurred by BAMS. (Doc. 22 at 10.) Also, Federal argues that the ADC Operational Recovery fee does not qualify as **Privacy Notification Expenses** because there is no evidence that the fee was used to “notify[] those **Persons** who may be directly affected by the potential

or actual unauthorized access of a **Record**, and changing such **Person's** account numbers, other identification numbers and security codes.” (Id.)

Chang's counters, stating that Federal's interpretation of “incur” is too narrow, as the Arizona Supreme Court held that an insured “incurs” an expense when the insured becomes liable for the expense, “even if the expenses in question were paid by or even required by law to be paid by other sources.” (Doc. 36 at 8 (citing *Samsel*, 204 Ariz. at 4-11, 59 P.3d at 284-91)).

The Court agrees with Chang's. Although the ADC Operational Reimbursement fee was originally incurred by BAMS, Chang's is liable for it pursuant to its MSA with BAMS.

In response to Federal's argument that there is no evidence that the ADC Operational Reimbursement fee was used to compensate Issuers for the costs of notifying about the security compromise and reissuing credit cards to Chang's customers, Chang's argues that MasterCard's Security Rules clearly state that the ADC Operational Reimbursement fee is used for that purpose. (Docs. 36 at 8, 24-1 at 84-88.) Federal does not direct the Court's attention to and the Court is unable to find any evidence in the record where the ADC Operational Reimbursement fee was used for any other purpose. The evidence shows that MasterCard performed an investigation into the Chang's data breach and determined Assessments pursuant to the MasterCard Rules. MasterCard then furnished a Report to BAMS levying the ADC Operational Reimbursement fee against BAMS, which it paid and then imposed the Assessment upon Chang's. (Doc. 26-3.) The Court does not find this to be a question of fact more suitable for a jury, but rather can find as a matter of law that coverage exists for the ADC Operational Reimbursement under Insuring Clause B. However, this finding is subject to the Court's analysis of the Policy's exclusions discussed below.

C. Insuring Clause D.2.

Under Insuring Clause D.2., “[Federal] shall pay...**Extra Expenses** an **Insured** incurs during the **Period of Recovery of Services** due to the actual or potential impairment or denial of **Operations** resulting directly from **Fraudulent Access or Transmission**.” (Doc. 8-1.) **Extra Expenses** include “reasonable expenses an **Insured** incurs in an attempt to continue **Operations** that are over and above the expenses such **Insured** would have normally incurred.

Extra Expenses do not include any costs of updating, upgrading or remediation of an **Insured's System** that are not otherwise covered under [the] Policy.” (Id.) In the context of **Extra Expenses**, **Period of Recovery of Services** “begins:...immediately after the actual or potential impairment or denial of **Operations** occurs; and will continue until the earlier of...the date **Operations** are restored,...to the condition that would have existed had there been no impairment or denial; or sixty (60) days after the date an **Insured's Services** are fully restored...to the level that would have existed had there been no impairment or denial.” (Id.) **Operations** are an **Insured's** business activities, while **Services** are “computer time, data processing, or storage functions or other uses of an **Insured's System**.” (Id.) **Fraudulent Access or Transmission** occurs when “a person has: fraudulently accessed an **Insured's System** without authorization; **Exceeded Authorized Access**; or launched a **Cyber-attack** into an **Insured's System**.” (Id.)

*7 Federal claims that Insuring Clause D.2. does not cover the Case Management Fee because Chang's has not submitted any evidence that the data breach caused “actual or potential impairment or denial” of business activities. (Doc. 22 at 11.) Chang's response states that the evidence clearly shows that its ability to operate was impaired because BAMS would have terminated the MSA and eliminated Chang's ability to process credit card transactions if it did not pay BAMS pursuant to the BAMS Letter. (Docs. 36 at 10, 23-2.) The MSA provides that Chang's is not permitted to use another servicer while contracting with BAMS for its services. (Doc. 23-2 at 3.) Furthermore, in her deposition, the approving underwriter for Federal, Leah Montgomery, states that she knew Chang's transacted much of its business through credit card payments and that Chang's would be adversely affected if it was unable to collect payment from credit card transactions. (Doc. 37-1 at 29.)

After reviewing the record, the Court agrees with Chang's. The evidence shows that Chang's experienced a **Fraudulent Access** during the data breach and that its ability to perform its regular business activities would be potentially impaired if it did not immediately pay the Case Management Fee imposed by BAMS. And, this Case Management Fee qualifies as an **Extra Expense** as contemplated by the Policy.

However, Federal argues that Chang's did not incur this **Loss** during the **Period of Recovery of Services** because it did not pay the Case Management Fee until April 15, 2015, nearly one year after it discovered the data breach. (Doc. 22

at 11.) Federal argues that because Chang's paid the Case Management Fee when it did, it falls outside the **Period of Recovery of Services**, which “begins:... immediately after the actual or potential impairment or denial of **Operations** occurs; and will continue until the earlier of...the date **Operations** are restored,...to the condition that would have existed had there been no impairment or denial; or sixty (60) days after the date an **Insured's Services** are fully restored...to the level that would have existed had there been no impairment or denial.” (Doc. 8-1.) In response, Chang's contends that its business activities are still not fully restored and that it continues to take steps to remedy the data breach; thus, the **Period of Recovery of Services** is ongoing. (Doc. 36 at 11.) Because this is an issue of fact, the Court is unable to resolve it on Summary Judgment. Accordingly, the Court cannot determine as a matter of law whether the Policy provides coverage for the Case Management Fee under Insuring Clause D.2.

D. Exclusions D.3.b. and B.2. and Loss Definition

Federal also argues that Exclusions D.3.b. and B.2, as well as the definition of **Loss**, bar coverage for all of the Assessments. Exclusion D.3.b. provides, “With respect to all Insuring Clauses, [Federal] shall not be liable for any **Loss** on account of any **Claim**, or for any **Expense**...based upon, arising from or in consequence of any...liability assumed by any **Insured** under any contract or agreement.” (Doc. 8-1.) Under Exclusion B.2., “With respect to Insuring Clauses B through H, [Federal] shall not be liable for...any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any **Insured**.” (Doc. 8-1.) Additionally, and along the same vein, **Loss** under Insuring Clause A does not include “any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any **Insured**.” (Id.) Functionally, these exclusions are the same in that they bar coverage for contractual obligations an insured assumes with a third-party outside of the Policy.

Federal contends that the assessments for which coverage is sought arise out of liability assumed by Chang's to BAMS, thus they are excluded from coverage. (Doc. 22 at 12.) Federal supports this argument by citing the MSA, wherein Chang's agreed that “[BAMS] may pass through to [Chang's] any fees assessed to [BAMS] by the Card Organizations, including but not limited to, new fees, fines, penalties and assessment[s].” (Doc. 23-1.) Federal also looks to the BAMS Letter where BAMS tells Chang's, “[i]n accordance with your Merchant Agreement you are obligated to reimburse [BAMS] for the...assessments.” (Doc. 23-8.)

*8 Chang's counters, offering a series of arguments why these exceptions are inapplicable in the present case. First, Chang's argues that such exclusions do not apply if "the insured is the one who is solely responsible for the injury," (citing 63 A.L.R.2d 1122 A.3d § 2[a]), or, in other words, the exclusions do not apply to obligations the insured is responsible for absent any assumption of liability. (Doc. 36 at 12) (citing Homeowners Mgmt. Enterp., Inc. v. Mid-Continent Cas. Co., 294 Fed.Appx. 814 821 (5th Cir. 2008) and Victoria's Secret Stores, Inc. v. Epstein Contracting, Inc., 2002 WL 723215, *4-5 (Ohio App. April 25, 2002)). Chang's argues that under the principal of equitable subrogation, it is compelled by "justice and good conscience," and not contractual liability, to compensate BAMS for the assessments. (Doc. 36 at 12) (citing Sourcecorp., Inc. v. Norcutt, 227 Ariz. 463, 466-67, 258 P.3d 281, 284-85 (App. 2011)). Chang's argues this is an exception recognized in the law to contractual liability exclusions of this nature. (*Id.*) Additionally, Chang's argues that its "responsibility for the Loss is the functional equivalent of compensating for damages suffered by victims of Privacy Injury, regardless of the MSA." (Doc. 36 at 12.) Under this argument, Chang's states that it could be liable under a variety of theories, including: negligence or particular statutes, such as A.R.S. § 44-7803, which places responsibility for fraudulent credit card transfers on merchants as opposed to credit card companies. (*Id.* at 12-13.) The Court is unconvinced by these arguments.

The Court finds that both Exclusions D.3.b. and B.2. as well as the definition of Loss bar coverage. In reaching this decision, the Court turned to cases analyzing commercial general liability insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same. Arizona courts, as well as those across the nation, hold that such contractual liability exclusions apply to "the assumption of another's liability, such as an agreement to indemnify or hold another harmless." Desert Mountain Properties Ltd. P'ship v. Liberty Mut. Fire Ins. Co., 225 Ariz. 194, 205, 236 P.3d 421, 432 (App. 2010), *aff'd*, 226 Ariz. 419, 250 P.3d 196 (2011) (citing Smithway Motor Xpress, Inc. v. Liberty Mut. Ins. Co., 484 N.W.2d 192, 196 (Iowa 1992)); *see also*, Gibbs M. Smith, Inc. v. U.S. Fid. & Guar. Co., 949 P.2d 337, 341 (Utah 1997); Lennar Corp. v. Great Am. Ins. Co., 200 S.W.3d 651, 693 (Tex. App. 2006).

Chang's agreement with BAMS meets this criteria and thus triggers the exclusions. In no less than three places in the MSA does Chang's agree to reimburse or compensate BAMS for any "fees," "fines," "penalties," or "assessments" imposed on BAMS by the Associations, or, in other words, indemnify BAMS. (See Doc. 23-2 at 9, 18.) More specifically, Section 13.5 of the Addendum to the MSA reads: "[Chang's] agrees to pay [BAMS] any fines, fees, or penalties imposed on [BAMS] by any Associations, resulting from Chargebacks and any other fines, fees or penalties imposed by an Association with respect to acts or omissions of [Chang's]." (*Id.* at 9.) Furthermore, the Court is unable to find and Chang's does not direct the Court's attention to any evidence in the record indicating that Chang's would have been liable for these Assessments absent its agreement with BAMS. While such an exception to an exclusion of this nature may exist in the law, it is not applicable here. Accordingly, the Court must find that the above referenced exclusions bar coverage for all three Assessments claimed by Chang's.

In reaching this conclusion, the Court has followed the dictate that "exclusionary clauses are interpreted narrowly against the insurer." Scottsdale Ins. Co., 158 Ariz. at 479, 763 P.2d at 543. Yet, even while looking through this deferential lens, the Court is unable to reach an alternative conclusion. Simply put, these exclusions unequivocally bar coverage for the Assessments, including the ADC Operational Reimbursement that the Court said coverage existed for under Insuring Clause B.

E. Reasonable Expectation Doctrine

Finally, the Court turns to Chang's claim that in addition to coverage being proper under the Policy, coverage also exists pursuant to the reasonable expectation doctrine. (Doc. 36 at 14.) The doctrine applies only if two predicate conditions are present. First, the insured's "expectation of coverage must be objectively reasonable." Miller, 167 Ariz. at 97, 804 P.2d at 826. Second, the insurer "must have had reason to believe that the [insured] would not have purchased the...policy if they had known that it included" the complained of provision. Grabowski, 214 Ariz. at 193-94, 150 P.3d at 280-81. Chang's bears the burden of proving the applicability of the reasonable expectation doctrine. *Id.*

*9 Thus, the starting point for the reasonable expectations analysis is "to determine what expectations have been induced." Darner, 140 Ariz. at 390, 682 P.2d at 395. Chang's states that the "dickered deal was for protection against losses resulting from [*sic*] a security compromise." (Doc. 36 at

15.) By this, Chang's means any and all fees and losses that flowed from the data breach, including the Assessments. Chang's directs the Court's attention to the deposition of Leah Montgomery, Federal's approving underwriter who renewed the Policy that was in effect at the time of the data breach. There, the evidence shows that when Federal issued the Policy it understood the realities associated with processing credit card transactions. (See Doc. 37-1.) Federal knew that all of Chang's credit card transactions were processed by a Servicer, such as BAMS, and the particular risks associated with credit card transactions. (Id. at 27, 85.) Federal also knew that Chang's, a member of the hospitality industry with a high volume of annual credit card transactions, was a higher risk entity and therefore paid a significant annual premium of \$134,052.00. (Id. at 29, 75, 126.) Federal was also aware that issuers will calculate Fraud Recovery and Operational Reimbursement Assessments against merchants in an effort to recoup losses suffered by security breaches. (Id. at 87-91.) Furthermore, Chang's also shows that Chubb markets the cyber security insurance policy as one that "address[es] the full breadth of risks associate with doing business in today's technology-dependent world" and that the policy "Covers direct loss, legal liability, and consequential loss resulting from cyber security breaches." (Doc. 37-7.)

Chang's then argues that based on all of the above, it possessed the expectation that coverage existed under the Policy for the assessments. But this is a *non sequitur* conclusion unsupported by the facts as presented. While Federal is aware of the realities of processing credit card transactions and that Chang's could very well be liable for Assessments from credit card associations passed through to them by Servicers, this does not prove what Chang's actual expectations were. Nowhere in the record is the Court able to find supporting evidence that during the underwriting process Chang's expected that coverage would exist for Assessments following a hypothetical data breach. There is no evidence showing that Chang's insurance agent, Kelly McCoy, asked Federal's underwriter if such Assessments would be covered during their correspondence. (See Doc. 37-5.) The cybersecurity policy application and related underwriting files are similarly devoid of any supporting evidence. (See Id.; Doc. 37-6.)

Chang's merely attempts to cobble together such an expectation after the fact, when in reality no expectation existed at the time it purchased the Policy. There is no evidence that Chang's bargained for coverage for potential Assessments, which it certainly could have done. Chang's and Federal are both sophisticated parties well versed in negotiating contractual claims, leading the Court to believe that they included in the Policy the terms they intended. See Taylor v. State Farm Mut. Auto. Ins. Co., 175 Ariz. 148, 158, 854 P.2d 1134, 1144 (1993); Tucson Imaging Associates, LLC v. Nw. Hosp., LLC, No. 2 CA-CV 2006-0125, 2007 WL 5556997, at *6 (Ariz. Ct. App. July 31, 2007). Because no expectation existed for this type of coverage, the Court is unable to find that Chang's meets its burden of satisfying the first predicate condition, objective reasonableness, to invoke the reasonable expectation doctrine. This obviates the need to analyze this issue further. Therefore, the Court finds that coverage likewise does not exist under the reasonable expectation doctrine.

IV. CONCLUSION

Accordingly, based on the foregoing reasons, **IT IS HEREBY ORDERED GRANTING** Defendant Federal Insurance Company's Motion for Summary Judgment. (Doc. 22.)

IT IS FURTHER ORDERED DENYING Plaintiff P.F. Chang's China Bistro, Inc.'s Unopposed Motion to Modify Case Schedule to Permit the Filing of an Amended Complaint (Doc. 44) as moot.

IT IS FURTHER ORDERED DISMISSING Plaintiff P.F. Chang's China Bistro, Inc.'s complaint with prejudice. The Clerk of Court shall enter judgment in favor of Defendant and terminate the case.

Dated this 26th day of May, 2016.

All Citations

Slip Copy, 2016 WL 3055111

101 F.Supp.3d 768
United States District Court,
S.D. Ohio,
Western Division.

Michael R. SCHMIDT, et al., Plaintiffs,
v.
The TRAVELERS INDEMNITY COMPANY OF
AMERICA, Defendant.

Case No. 1:13-cv-932.

Signed March 31, 2015.

Synopsis

Background: Insured law firm and lawyer brought action against insurer, alleging that insurer breached the parties' contract and acted in bad faith when it refused to indemnify the firm pursuant to its businessowners property **insurance** policy for losses incurred as a result of a fraudulent check scheme. Both parties moved for summary judgment.

Holdings: The District Court, Timothy S. Black, J., held that:

^[1] policy's "**voluntary parting**" **exclusion** applied to loss arising from lawyer's wiring of funds to client under false pretenses;

^[2] policy's "**default**" **exclusion** did not apply to any losses;

^[3] losses were not covered by policy's business personal property provision;

^[4] losses were not covered by policy's business income and extra expense provision.

Ordered accordingly.

West Headnotes (13)

^[1] **Insurance**
☞ Questions of law or fact

Under Ohio law, construing an **insurance** policy is a matter of law.

Cases that cite this headnote

^[2] **Insurance**
☞ Intention

In interpreting an **insurance** contract under Ohio law, the court gives effect to the intent of the parties to the agreement.

Cases that cite this headnote

^[3] **Insurance**
☞ Plain, ordinary or popular sense of language

In interpreting an **insurance** contract under Ohio law, the court gives words and phrases their ordinary meaning unless another meaning is apparent from the contents of the policy.

Cases that cite this headnote

^[4] **Insurance**
☞ Construction as a whole

In interpreting an **insurance** contract under Ohio law, the court gives meaning to every paragraph, clause, phrase, and word.

Cases that cite this headnote

^[5] **Insurance**
☞ Ambiguity, Uncertainty or Conflict
Insurance
☞ Necessity of ambiguity

Under Ohio law, if provisions in an insurance contract are reasonably susceptible of more than one meaning, they will be construed strictly against the insurer and liberally in favor of the insured; however, provisions are to be strictly construed against the insurer only when they are ambiguous.

Cases that cite this headnote

- [6] **Insurance**
⚡Construction or enforcement as written
Insurance
⚡Plain, ordinary or popular sense of language
Insurance
⚡Necessity of ambiguity

Under Ohio law, the general rule of liberal construction of insurance contracts in favor of the insured cannot be used to create an ambiguity where one does not exist; if the terms of a policy are clear and unambiguous, a court must enforce the contract as written, giving words used in the contract their plain and ordinary meaning.

Cases that cite this headnote

- [7] **Insurance**
⚡Duty to indemnify in general

Under Ohio law, an insurer's obligation to its insured arises only if the claim falls within the scope of coverage.

Cases that cite this headnote

- [8] **Insurance**
⚡Burden of proof

Under Ohio law, the party who seeks to recover under an insurance policy generally has the burden of demonstrating coverage under the policy and proving a loss; however, the insurer

bears the burden of proving that an exclusion applies.

Cases that cite this headnote

- [9] **Insurance**
⚡Exclusions and limitations in general
Insurance
⚡Presumptions

Under Ohio law, exclusionary language in insurance policies must be clear and exact; a general presumption arises to the effect that which is not clearly excluded from the operation of such contract is included in the operation thereof.

Cases that cite this headnote

- [10] **Insurance**
⚡Voluntary parting with possession

Under Ohio law, "voluntary parting" exclusion in businessowners property insurance policy applied to exclude insured law firm's loss claim arising from lawyer's wiring of funds to Japanese bank account of client purporting to be entitled to funds from settlement check cashed by firm, which firm discovered was fraudulent after the wire had been sent; fact that lawyer wired the money in reliance on misrepresentations or false pretenses did not alter the voluntariness of the parting.

Cases that cite this headnote

- [11] **Insurance**
⚡Risks or Losses Covered and Exclusions

Under Ohio law, "default" exclusion in businessowners property insurance policy did not apply to exclude insured law firm's loss claims arising from company's failure to honor its settlement checks and client's failure to

return funds that lawyer wired to him before the checks were discovered to be fraudulent; the losses were the clear result of fraud, not a knowing decision on the firm's part to extend credit to the defrauder.

Cases that cite this headnote

[12]

Insurance

⚙️Risks or Losses Covered and Exclusions

Under Ohio law, business personal property provision in businessowners property **insurance** policy did not apply to insured law firm's loss claim arising from company's failure to honor cashier's checks purportedly sent as part of a settlement with firm's client, which were discovered to be fraudulent after firm wired money to client; provision required direct physical loss or damage to covered property, and there was no indication that the checks were physically lost or damaged.

1 Cases that cite this headnote

[13]

Insurance

⚙️Business Interruption; Lost Profits

Under Ohio law, business income and extra expense provision in businessowners property **insurance** policy did not apply to insured law firm's loss claim arising from client's failure to return funds that were wired to him before the firm discovered that settlement checks purportedly intended to satisfy client's claims were fraudulent; there was no indication that firm's business activities underwent a partial or complete cessation or that it lost business income or incurred extra expense as a result of direct physical loss of or damage to property at its law offices.

Cases that cite this headnote

Attorneys and Law Firms

*770 Paul M. De Marco, Terence Richard Coates, Christopher D. Stock, Markovits, Stock & Demarco LLC, Cincinnati, OH, for Plaintiffs.

D. John Travis, Gary L. Nicholson, Melanie R. Shaerban, Gallagher, Sharp, Fulton & Norman, Cleveland, OH, for Defendant.

**ORDER GRANTING DEFENDANT'S MOTION
FOR PARTIAL SUMMARY JUDGMENT (Doc. 8)
AND DENYING PLAINTIFFS' MOTION FOR
PARTIAL SUMMARY JUDGMENT (Doc. 9)**

TIMOTHY S. BLACK, District Judge.

This civil action is before the Court on the parties' cross motions for partial summary judgment (Docs. 8, 9) and responsive memoranda (Docs. 14, 15, 16, 17).

I. BACKGROUND FACTS

Plaintiffs Michael R. Schmidt ("Schmidt") and Cohen, Todd, Kite & Stanford LLC ("CTKS") allege that Defendant Travelers Indemnity Company of America ("Travelers") breached the parties' contract and acted in bad faith when it refused to indemnify Plaintiff CTKS pursuant to an **insurance** policy. (*See* Doc. 1 at ¶¶ 34–39, 42–47). In addition to damages and attorney's fees, Plaintiffs seek a declaration that the loss is a covered loss under the policy and, therefore, Defendant owes Plaintiff CTKS a duty of indemnification. (*See id.* at ¶¶ 40–41).

Plaintiffs and Defendant filed cross-motions for partial summary judgment.¹ *771 Plaintiffs argue that Defendant breached its obligations under the **insurance** policy then in effect (the "Policy") by refusing to pay Plaintiff CTKS for its covered losses. Defendant argues that the Policy does not cover the loss sustained and, in any event, the loss is specifically excluded.²

II. UNDISPUTED FACTS

A. In Support of Plaintiffs' Motion for Partial Summary Judgment³

1. CTKS paid **insurance** premiums to Travelers in exchange for which Travelers provided business owners **insurance** coverage to CTKS under Policy No. 1-680-9A246743-TIA-11 ("Policy"). (Doc. 9-1 at 2, ¶ 1; Doc. 1-3 at 2-3).

2. As a result of CTKS's payment of the **insurance** premiums when due, the Policy was in effect from December 14, 2011 through December 14, 2012. (Doc. 9-1 at 2-3, ¶ 2; Doc. 1-3 at 2-3).

3. The Policy contains a "Computer Fraud" provision stating that **insurance** may be extended "to apply to loss of or damage to Business Personal Property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the building at the described premises or 'banking premises': (a) To a person outside those premises; or (b) To a place outside those premises." (Doc. 9-1 at 6, ¶ 13; *see also* Doc. 1-4 at 26).

4. On February 21, 2012, while the Policy was in effect, Schmidt received an **email** on his CTKS computer requesting legal representation from a person purporting to be Erick Carpenter, supposedly a resident of Japan. (Doc. 9-1 at 4, 6, ¶¶ 3, 14; *see also* at Doc. 9-2 at ¶¶ 2-3, 28).

5. On February 27, 2012, Plaintiffs and the person purporting to be Erick Carpenter entered into a retention agreement via **electronic mail**, whereby Plaintiffs undertook to represent the purported Erick Carpenter with respect to his claims against North American Iron and Steel Company ("North American"), in exchange for a 25 percent contingent fee. (Doc. 9-2 at ¶¶ 6, 28; Doc. 9-1 at 4, 7, ¶¶ 4, 15; *see also* Doc. 1-1 at 2-5).

6. The person purporting to be Erick Carpenter then provided Schmidt with additional details regarding his purported claim against North

American via **electronic mail**. (Doc. 9-2 at ¶¶ 5, 28; *see also* Doc. 9-1 at 7, ¶ 16).

7. After entering into the retention agreement, Schmidt drafted a demand letter to North American and forwarded the draft to the person purporting to be Erick Carpenter through the use of a computer. (Doc. 9-2 at ¶¶ 7-8, 28; *see also* Doc. 9-1 at 7, ¶¶ 17-18).

8. In response to Schmidt's **email**, the purported Erick Carpenter sent his approval of the draft letter to Schmidt via **electronic mail**. (Doc. 9-2 at ¶¶ 9, 28; *see also* Doc. 9-1 at 8, ¶ 19).

9. On February 29, 2012, Schmidt sent a letter to North American via **electronic mail** using his CTKS computer. (Doc. 9-2 at ¶¶ 10, 28; *see also* Doc. 9-1 at 4, 8, ¶¶ 4, 20).

10. The letter, which was sent to an **email** address that the purported Erick Carpenter had provided, demanded payment of \$378,000 to Schmidt as counsel for Carpenter. (Doc. 9-2 at *772 ¶¶ 10, 28; *see also* Doc. 9-1 at 4, 8, ¶¶ 4, 20).

11. Also on February 29, 2012, a person purporting to be Edgar Marshall, on behalf of North American, responded to Schmidt's demand letter, also via **email**. (Doc. 9-2 at ¶¶ 11, 28; *see also* Doc. 9-1 at 8, ¶ 21).

12. In the **email** to Schmidt, the purported Edgar Marshall offered that North American would pay the balance of the outstanding \$378,000 supposedly owed to Erick Carpenter and would do so in two separate \$189,000 payments. (Doc. 9-2 at ¶¶ 12, 28).

13. Schmidt conveyed that offer to the person purporting to be Erick Carpenter via **electronic mail** using his computer. (Doc. 9-2 at ¶¶ 13, 28; *see also* Doc. 9-1 at 8, ¶ 22).

14. Via **electronic mail**, the person purporting to be Erick Carpenter sent his authorization to Schmidt to accept the offer made by Edgar Marshall. (Doc. 9-1 at 9, ¶ 23; *see also* Doc. 9-2 at ¶¶ 14, 28).

15. Via **electronic mail** and through the use of his computer, Schmidt conveyed to the person purporting to be Edgar Marshall that Erick Carpenter had accepted Marshall's offer. (Doc. 9-1 at 9, ¶ 24; *see also* Doc. 9-2 at ¶¶ 15, 28).

16. Following these communications, all of which took place via **electronic mail**, CTKS received what purported to be a cashier's check in the amount of \$189,000 from North American on March 6, 2012. (Doc. 9-1 at 4-5, ¶ 6; *see also* Doc. 9-2 at ¶¶ 16, 28).

17. The person purporting to be Erick Carpenter, via **electronic mail**, transmitted instructions to Schmidt for wiring \$141,750 (\$189,000 minus CTKS's 25 percent contingent fee) to Carpenter's account in Japan. (Doc. 9-1 at 9, ¶ 25; *see also* Doc. 9-2 at ¶¶ 18, 28).

18. Plaintiffs deposited the purported \$189,000 cashier's check into CTKS's IOLTA account. (Doc. 9-2 at ¶ 17).

19. On March 7, 2012, CTKS wired \$141,750 to the Japanese bank account of the person purporting to be Erick Carpenter, as instructed. (*Id.* at ¶ 19).

20. Only after wiring the amount of \$141,750 did Plaintiffs learn from their own bank that the cashier's check they received from North American and then deposited was fraudulent. (*Id.* at ¶ 20).

21. A second cashier's check for \$189,000 from North American, which Plaintiffs received on March 12, 2012, also was fraudulent. (*Id.*)

22. On March 14, 2012, more than a week after Plaintiffs wired the amount of \$141,750 to the account of the person purporting to be Erick Carpenter and learned that the purported cashier's checks from North American were fraudulent, the person purporting to be Erick Carpenter, via **electronic mail**, separately informed Schmidt that he would send a check for \$141,750 to Schmidt. (Doc. 9-1 at 10, ¶ 26; *see also* Doc. 9-2 at ¶¶ 21, 28).

23. Plaintiffs have received no money back from the person or persons purporting to be Erick Carpenter or Edgar Marshall. (Doc. 9-2 at ¶ 22).

24. CTKS, through its Cincinnati **insurance** agent, Neace Lukens, filed a timely claim for its losses with Travelers in the amount of \$141,750, asserting that its losses should be covered under the Policy. (Doc. 9-1 at 5, ¶ 8; *see also* Doc. 9-2 at ¶¶ 24, 26).

25. CTKS later submitted to Travelers additional information supporting its claim for **insurance** coverage. Travelers denied CTKS's claim for coverage *773 in letters dated April 17, 2012 and May 2, 2012. (Doc. 9-1 at 5, ¶ 10; *see also* Doc. 9-2 at ¶ 27).

26. In a January 7, 2013 letter, Travelers again denied CTKS's claim for **insurance** coverage under the Policy. (Doc. 9-1 at 5, ¶ 9; *see also* Doc. 9-2 at ¶ 27).

B. In Support of Defendant's Motion for Partial Summary Judgment⁴

1. Plaintiffs Michael R. Schmidt ("Schmidt") and Cohen, Todd, Kite & Stanford LLC ("CTKS") seek indemnification from Defendant Travelers Indemnity Company of America ("Travelers") for the loss CTKS sustained when Schmidt, acting on behalf of CTKS, wired \$141,750 from CTKS's IOLTA (trust) account at Chase Bank to Erick Carpenter's bank account in Japan ("\$141,750 Loss"). (Doc. 1 at ¶¶ 21-27, 33).⁵

2. Schmidt, a member of CTKS licensed to practice law in the State of Ohio, agreed on behalf of CTKS to represent Erick Carpenter relating to a purported breach of a settlement agreement between Carpenter and his former employer, North American Iron and Steel Company ("North American"). (*Id.* at ¶¶ 2, 9, 12).

3. Schmidt drafted and emailed a letter to North American demanding that it pay the balance owed on the purported settlement agreement (\$378,000), and a person purportedly acting on behalf of North America (Edgar Marshall) offered to make a payment of \$378,000 to Carpenter in two installments of \$189,000. (*Id.* at ¶¶ 13, 16, 17).

4. Schmidt emailed Erick Carpenter's acceptance of Edgar Marshall's offer, and on March 6, 2012 Schmidt received what appeared to be a cashier's check in the amount of \$189,000 from North American ("North American Check"). (*Id.* at ¶¶ 20, 21).

5. Schmidt deposited the North American Check into CTKS's IOLTA (trust) account at Chase Bank, deducted CTKS's twenty-five percent contingent fee, and wired the balance of \$141,750 to Erick Carpenter's bank account in

Japan, account no. 1017380 ("Wire Transfer"). (*Id.* at ¶¶ 22, 23).

6. After the Wire Transfer was complete, Chase Bank notified CTKS, and Schmidt learned, that the North American Check had been dishonored as fraudulent. (*Id.* at ¶ 24).

7. After Schmidt learned that the North American Check had been dishonored, Schmidt left Edgar Marshall telephone messages notifying North American that the North American Check was dishonored, and sent Erick Carpenter an email demanding that he return the \$141,750 that Schmidt wired to Erick Carpenter's bank account. (*Id.* at ¶¶ 25, 26).

8. Edgar Marshall did not respond to Schmidt's telephone messages, and Erick Carpenter failed to return any of the \$141,750 that Schmidt wired to Erick Carpenter's bank account. (*Id.* at ¶¶ 25–27).

9. Travelers issued policy number I-680-9A246743-TIA-11 ("Policy") to CTKS, an Ohio insured, in Ohio. (*Id.* at ¶ 5).

*774 10. The Policy contains Common Policy Declarations, a Businessowners Property Coverage Special Form, and a Lawyers Endorsement. (See Doc. 8–2; see also Doc. 8–3 at 29–169).⁶

11. In the introductory paragraphs of the Businessowners Property Coverage Special Form, it is stated that: "Throughout this policy the words 'you' and 'your' refer to the Named Insured shown in the Declarations [CTKS]. The words 'we', 'us' and 'our' refer to the Company providing this insurance [Travelers]." (Doc. 8–2 at 2).

12. Paragraph A. of the "COVERAGE" of the Policy's Businessowners Property Coverage Special Form states, "We [Travelers] will pay for direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from a Covered Cause of Loss." (*Id.*)

13. "Covered Property" is stated to be "the type of property described in this Paragraph A.1., and limited in Paragraph A.2., Property Not Covered, if a Limit of Insurance is shown in the Declarations for that type of property." (*Id.*)

14. The "described premises" are CTKS's law offices at 250 E. 5th Street, Suite 1200, Cincinnati,

Ohio. (*Id.* at 1).

15. The \$141,750 Loss was to CTKS's IOLTA (trust) account. (Doc. 1 at ¶ 23).⁸

16. Paragraph A. of the "COVERAGE" of the Businessowners Property Coverage Special Form requires "direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from a Covered Cause of Loss". (Doc. 8–2 at 2).⁹

17. "Covered Causes of Loss" is "DIRECT PHYSICAL LOSS unless the loss is ... b. Excluded in Paragraph B., Exclusions." (*Id.* at 4–5).¹⁰

18. The Lawyers Endorsement of the Policy "modifies insurance provided under the ... BUSINESSOWNERS PROPERTY COVERAGE SPECIAL FORM". (*Id.* at 42).

19. The following Coverage Extension is added by the Lawyers Endorsement:

b. Computer Fraud

(1) When a Limit is shown in the Declarations for Business Personal Property at the described premises, *775 you [CTKS] may extend that insurance to apply to loss of or damage to Business Personal Property resulting directly from the use of any computer to fraudulently cause a transfer of the property from the inside the building at the described premises or "banking premises":

(a) To a person outside those premises; or

(b) To a place outside those premises.

(2) Paragraph B.2.o. does not apply to this Coverage Extension.

(3) The most we will pay under this Coverage Extension in any one occurrence is \$10,000, regardless of the number of premises involved.

(*Id.* at 45).

20. Subsection 2. of Paragraph B., Exclusions, states that: "2. We [Travelers] will not pay for loss or damage caused by or resulting from any of the following: ... i. Voluntary parting with any property by you [CTKS] or anyone else to whom you have entrusted the property", or "I. Default on any credit sale, loan, or similar transaction." (*Id.* at 25–26).¹¹

21. The Lawyers Endorsement does not provide that

these exclusions, Paragraphs B.2.i. and B.2.l., are inapplicable to the Computer Fraud Coverage Extension. (*Id.*)¹²

III. STANDARD OF REVIEW

A motion for summary judgment should be granted if the evidence submitted to the Court demonstrates that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law. Fed.R.Civ.P. 56(c). See *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247–48, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). The moving party has the burden of showing the absence of genuine disputes over facts which, under the substantive law governing the issue, might affect the outcome of the action. *Celotex*, 477 U.S. at 323, 106 S.Ct. 2548. All facts and inferences must be construed in a light most favorable to the party opposing the motion. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986).

A party opposing a motion for summary judgment “may not rest upon the mere allegations or denials of his pleading, but ... must set forth specific facts showing that there is a genuine issue for trial.” *Anderson*, 477 U.S. at 248, 106 S.Ct. 2505 (1986).

IV. ANALYSIS

Plaintiffs invoke three policy provisions in support of their motion for summary judgment on the coverage issue: (1) the Computer Fraud coverage extension; (2) the Business Personal Property provision; and (3) the Business Income and Extra Expense provision.¹³ Defendant argues *776 that these provisions do not cover the loss suffered by Plaintiff CTKS and, in any event, “voluntary parting” and “default” coverage exclusions apply.

[1] [2] [3] [4] The parties agree that Ohio law applies. (See Doc. 8–1 at 10–11).¹⁴ Construing an insurance policy is a matter of law. See *Alexander v. Buckeye Pipe Line Co.*, 53 Ohio St.2d 241, 245–46, 374 N.E.2d 146 (1978). In interpreting an insurance contract, the Court gives effect to the intent of the parties to the agreement. *Hamilton Ins.*

Serv., Inc. v. Nationwide Ins. Cos., 86 Ohio St.3d 270, 273, 714 N.E.2d 898 (1999) (citation omitted). The Court gives words and phrases their ordinary meaning unless another meaning is apparent from the contents of the policy. *Westfield Ins. Co. v. Galatis*, 100 Ohio St.3d 216, 219, 797 N.E.2d 1256 (2003) (citing *Alexander*, 53 Ohio St.2d at 241, 374 N.E.2d 146). The Court gives meaning to every paragraph, clause, phrase, and word. *Affiliated FM Ins. Co. v. Owens-Corning Fiberglas Corp.*, 16 F.3d 684, 686 (6th Cir.1994) (citing *Heifner v. Swaney*, 1992 WL 198120 (Ohio App. Aug. 27, 1992)).

[5] [6] If provisions are reasonably susceptible of more than one meaning, they “will be construed strictly against the insurer and liberally in favor of the insured.” *King v. Nationwide Ins. Co.*, 35 Ohio St.3d 208, 519 N.E.2d 1380 (1988), syllabus. However, provisions are to be strictly construed against the insurer only when they are ambiguous. *GenCorp, Inc. v. Am. Intern. Underwriters*, 178 F.3d 804, 818 (6th Cir.1999) (citing *University of Cincinnati v. Arkwright Mut. Ins. Co.*, 51 F.3d 1277, 1280 (6th Cir.1995) (applying Ohio law)). “[T]he general rule of liberal construction cannot be used to create an ambiguity where one does not exist. If the terms of a policy are clear and unambiguous, a court must enforce the contract as written, giving words used in the contract their plain and ordinary meaning.” *Monticello Ins. Co. v. Hale*, 284 F.Supp.2d 898, 901 (S.D. Ohio 2003) (citations omitted).

[7] [8] [9] “A liability insurer’s obligation to its insured arises only if the claim falls within the scope of coverage.” *Cincinnati Indem. Co. v. Martin*, 85 Ohio St.3d 604, 605, 710 N.E.2d 677 (1999). The party who seeks to recover under an insurance policy generally has the burden of demonstrating coverage under the policy and proving a loss. *Chicago Title Ins. Co. v. Huntington Nat’l Bank*, 87 Ohio St.3d 270, 273, 719 N.E.2d 955 (1999) (citing *Inland Rivers Service Corp. v. Hartford Fire Ins. Co.*, 66 Ohio St.2d 32, 418 N.E.2d 1381 (1981)). However, the insurer bears the burden of proving that an exclusion applies. *Cont’l Ins. Co. v. Louis Marx Co.*, 64 Ohio St.2d 399, 415 N.E.2d 315, 317 (1980). Exclusionary language in insurance policies must be clear and exact. See *Lane v. Grange Mut. Cos.*, 45 Ohio St.3d 63, 65, 543 N.E.2d 488 (1989). “A general presumption arises to the effect that that which is not clearly excluded from the operation of such contract is included in the operation thereof.” *King*, 35 Ohio St.3d at 214, 519 N.E.2d 1380.

A. Claimed Losses

Plaintiffs claim to have suffered three distinct covered losses, each of which must be analyzed separately: (1) loss because the cashier's checks they received from North American were fraudulent ("First *777 Loss"); (2) loss because Plaintiffs wired \$141,750 to the person purporting to be Erick Carpenter ("Second Loss"); and (3) loss because the person purporting to be Erick Carpenter failed to pay \$141,750 to Plaintiffs as promised ("Third Loss"). Defendant argues that Plaintiffs suffered a single loss, which occurred when they wired \$141,750 from Plaintiff CTKS's IOLTA account at Chase Bank to Erick Carpenter's bank account in Japan. Defendant claims that Plaintiffs had not described their loss as "three distinct covered losses" prior to filing their cross-motion for partial summary judgment and argues that, while every loss can be viewed from different perspectives, those different perspectives do not transform a single loss into multiple losses.

The Court finds that Plaintiffs' claimed losses are supported by the undisputed facts.¹⁵ Accordingly, and in the absence of any authority requiring the Court to construe Plaintiffs' claimed losses as a single loss, the Court will determine whether any of the three claimed losses were covered under the Policy.

B. Exclusions

Defendant claims that Plaintiffs' claimed losses are clearly and unambiguously excluded from coverage under the Policy. Because the Court finds that the "voluntary parting" exclusion clearly and unambiguously excludes Plaintiffs' Second Loss, and thereby renders analysis of whether the Computer Fraud coverage extension applies to such a loss unnecessary, the Court will address the exclusions first. The Businessowners Property Coverage Special Form states, in relevant part, as follows:

B. EXCLUSIONS

...

2. We will not pay for loss or damage caused by or resulting from any of the following:

...

i. **Voluntary parting** with any property by you or anyone else to whom you have entrusted the property.

...

1. Default on any credit sale, loan, or similar transaction.

(Doc. 8–2 at 23, 24–25).

1. Voluntary Parting Exclusion

^[10] Courts that have considered exclusions similar to the instant "voluntary parting" exclusion have found that these exclusions are conspicuous, plain, and clear. For example, in *Martin, Shudt, Wallace, DiLorenzo & Johnson v. Travelers Indem. Co. of Conn.*, No. 1:13-cv-0498, 2014 WL 460045 (N.D.N.Y. Feb. 5, 2014), the court considered facts similar to those in the instant case and dismissed the insured's claims based on similar "voluntary parting" language.¹⁶ There, the insured law firm sought coverage for a loss it incurred after wiring funds to a purported overseas client, having subsequently discovered that a cashier's check thought to represent a payment of funds owed to that client, *778 which the insured had deposited into its trust account, was fraudulent. *Id.* at *1.

The court in *Martin* held that the "voluntary parting" exclusion applied, despite the fact that the insured was tricked into directing the wire transfer. *Martin*, 2014 WL 460045, at *3 ("On its face, the **Voluntary Parting Exclusion** unambiguously encompasses Plaintiff's Loss."). As the court explained: "[t]hat Plaintiff wired the money in reliance on misrepresentations or false pretenses does not alter the voluntariness of that parting."¹⁷ The court rejected the insured's argument that Travelers' "voluntary parting" exclusion was ambiguous and that the exclusion "could reasonably be interpreted to encompass only gifts, loans, or bailments of property." *Id.* at *4.¹⁸ The Court finds this decision in *Martin* to be highly persuasive here.

Plaintiffs argue that the presence of fraud vitiated their ability to voluntarily part with the funds wired. In support of their contention, they cite to Ohio case law establishing that a payment induced by fraud is not treated as a voluntary payment.¹⁹ However, these cases address *779 only whether recovery may be had from the parties who received such payments and not whether the payors voluntarily *parted with* the funds.²⁰ Accordingly, based on the foregoing, the Court finds that Plaintiffs' Second Loss is clearly excluded by the "voluntary parting" provision.²¹

2. Default Exclusion

^[11] Defendant summarily concludes that the Court may hold that the “default” exclusion bars Plaintiff CTKS’s recovery of the losses it incurred because North American failed to honor its checks (First Loss) and because Carpenter failed to return the \$141,750.00 that Plaintiff Schmidt wired to him (Third Loss).

Defendant fails to explain in what respect North American’s transmission of two fake cashier’s checks or the purported Erick Carpenter’s failure to pay \$141,750 to Plaintiff Schmidt as promised constitute a “default” on a “credit sale, loan, or similar transaction.” North American sent the two fake cashier’s checks purportedly to fulfill a settlement agreement, not to pay off a loan that Plaintiff CTKS had made to North American. Further, the person purporting to be Carpenter reneged on a promise to send Plaintiff Schmidt \$141,750, and there is no evidence that Plaintiffs made a loan or entered into a credit transaction with Carpenter requiring him to send \$141,750 to the Plaintiffs.

*780 In *Bank of Ann Arbor v. Everest Nat’l Ins. Co.*, 563 Fed.Appx. 473, 477–78 (6th Cir.2014), the Sixth Circuit rejected a similar attempt by an insurer to deny coverage based on a “loan loss” provision invoked under similar circumstances. There, the plaintiff bank sought coverage after being defrauded by means of a fake wire transfer request from an impostor posing as one of its customers. The bank lost almost \$200,000 by wiring such amount from the true customer’s account to that of the impostor in Korea. The Sixth Circuit stated:

Defendant contends that the loss Plaintiff suffered as a result of the fraudulent wire transfer request was from the extension of credit and is therefore excluded from coverage. However, the clear meaning of section 2(e) is that Defendant will not cover a loss resulting from a customer default on a loan or extension of credit made by Plaintiff. The loss in this case did not result from the nonpayment of a loan. It was a loss as a result of a fraudulent wire transfer request by someone other than the true customer.

Here, as in *Bank of Ann Arbor*, the losses for which the insurer invokes this exclusion were the clear result of fraud, not a knowing decision on the insured’s part to

extend credit to the defrauder. For these reasons, the Court finds that the “default” provision does *not* clearly exclude Plaintiffs’ First or Third Losses. Accordingly, it will analyze the applicability of the coverage provisions invoked by Plaintiffs to these losses.

C. Policy Coverage

1. Business Personal Property Provision

^[12] Plaintiffs argue that their First Loss is covered under the Business Personal Property provision. The Businessowners Property Coverage Special Form provides, in relevant part, as follows:

A. COVERAGE

We will pay for direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from a Covered Cause of Loss.

1. Covered Property

Covered Property, as used in this Coverage Form, means the type of property described in this Paragraph A.1, and limited in Paragraph A.2., Property Not Covered, if a Limit of Insurance is shown in the Declarations for that type of property....

b. Business Personal Property located in or on the buildings described in the Declarations or in the open (or in a vehicle) within 1,000 feet of the described premises, including: ...

(4) “Money” and “Securities”....

4. Covered Causes of Loss

RISKS OF DIRECT PHYSICAL LOSS unless the loss is:

a. Limited in Paragraph A.5, Limitations; or

b. Excluded in Paragraph B., Exclusions.

(Doc. 8–2 at 2, 4–5).²²

Plaintiffs argue that the purported cashier’s checks

received from North American are “business personal property” because they fit within the Policy’s definition of “securities.” (See Doc. 8–2 at 39) (defining “securities” as “all negotiable and non-negotiable instruments or contracts representing either ‘money’ or other property”). *781 Plaintiffs explain that, like “securities,” cashier’s checks are negotiable instruments that represent money. Plaintiffs note that the terms “direct physical loss” and “covered cause of loss” are not explicitly defined and argue that, as a result, the provision is ambiguous.

The Court need not reach the question of whether the purported cashier’s checks are “business personal property,” and, thereby, “covered property,” because there was no “direct physical loss of or damage to” the “checks.” The Policy requires “direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from a Covered Cause of Loss” and thereafter states that “Covered Causes of Loss” are “DIRECT PHYSICAL LOSS unless the loss is” limited or excluded. This is *not* an instance in which, for example, cashier’s checks were destroyed and lost in a fire.²³ Because Plaintiff has not presented evidence that the purported cashier’s checks were physically lost or damaged, the Court finds that the First Loss is not covered loss under the Business Personal Property provision.

2. Business Income and Extra Expense Provision

[²³] Plaintiffs argue that their Third Loss, combined with the loss sustained by the dishonoring of the second cashier’s check, is covered under the Business Income and Extra Expense provision of the Policy. The Businessowners Property Coverage Special Form states, in relevant part, as follows:

A. COVERAGE

...

3. Business Income and Extra Expense

Business Income and Extra Expense is provided at the premises described in the Declarations when the Declarations show that you have coverage for Business Income and Extra Expense.

a. Business Income

(1) Business Income means:

(a) Net Income (Net Profit or Loss before income taxes) that would have been earned or incurred ... and

(b) Continuing normal operating expenses incurred, including payroll.

(2) We will pay for the actual loss of Business Income you sustain due to the necessary “suspension” of your “operations” during the “period of restoration.” The “suspension” must be caused by direct physical loss of or damage to property at the described premises. The loss or damage must be caused by or result from a Covered Cause of Loss....

*782 b. Extra Expense

(1) Extra Expense means reasonable and necessary expenses you incur during the “period of restoration” that you would not have incurred if there had been no direct physical loss of or damage to property caused by or resulting from a Covered Cause of Loss.

(2) We will pay Extra Expense (other than the expense to repair or replace property) to:

(a) Avoid or minimize the “suspension” of business and to continue “operations” at the described premises or at replacement premises or temporary locations, including relocation expenses and costs to equip and operate the replacement premises or temporary locations; or

(b) Minimize the “suspension” of business if you cannot continue operations.

(3) We will also pay Extra Expense (including Expediting Expenses) to repair or replace the property, but only to the extent it reduces the amount of loss that otherwise would have been payable under Paragraph a. Business Income, above.

(Doc. 8–2 at 3–4).²⁴ “Suspension” is defined as “[t]he partial or complete cessation of your [CTKS’s] business activities” or “[t]hat a part or all of the described premises is rendered untenable.” (*Id.* at 40). “Operations” is defined as “your [CTKS’s] business activities occurring at the described premises and the tenantability of the described premises.” (*Id.* at 38).

Plaintiffs explain that, as a consequence of the wiring of the \$141,750 to the purported Erick Carpenter’s account in Japan and the dishonoring of the first cashier’s check

from North American, they were forced to incur the added expense of depositing \$141,750 into Plaintiff CTKS's IOLTA account to restore the account's balance, pending the receipt of the check the purported Erick Carpenter promised to send and the second North American cashier's check. Because Carpenter never sent his check and the second cashier's check was dishonored as fraudulent, Plaintiffs never recovered their deposit. Plaintiffs argue that, for a law firm, having an IOLTA account balance short by \$141,750 constitutes a definite and significant interruption of the law firm's normal business activities. Plaintiffs claim that their loss of \$141,750 should be treated as an "Extra Expense" covered under the Policy. They also argue that not enjoying the benefits of the check that Carpenter failed to send or of the second North American cashier's check should be treated as lost "Business Income," also covered under the Policy.

The Court cannot agree that the losses described are covered. Plaintiffs suffered no loss of income due to the necessary "suspension" of their "operations" *"caused by a direct physical loss of or damage to property at the described premises [CTKS's law offices]"*. (Doc 8-2 at 3-4) (emphasis supplied). Further, the coverage provided for an insured's Extra Expense does not cover Plaintiffs' loss because the expenses incurred did not follow a *"direct physical loss of or damage to property caused by or resulting from a Covered Cause of Loss."* (Doc 8-2 at 38) (emphasis added).²³ Plaintiffs have not presented evidence that their business activities underwent a partial or complete cessation or that they lost business income or

incurred extra expense as a result direct physical loss of or damage to property *783 at the described premises. The Court finds that Plaintiffs' Third Loss, combined with the loss sustained by the dishonoring of the second cashier's check, is not a covered loss.

V. CONCLUSION

For the foregoing reasons, the Court finds that Plaintiffs' claimed losses were not covered under the Policy. Accordingly:

1. Defendant's motion for partial summary judgment as to Plaintiffs' breach of contract and declaratory judgment claims (Doc. 8) is **GRANTED**;
2. Plaintiffs' motion for partial summary judgment as to their breach of contract claim (Doc. 9) is **DENIED**.

IT IS SO ORDERED.

All Citations

101 F.Supp.3d 768

Footnotes

- ¹ The Court bifurcated the coverage and bad faith issues. (See March 12, 2014 Minute Entry and Notation Order). Accordingly, only the coverage issue is now before the Court. Plaintiffs seek summary judgment as to their breach of contract claim (Count One); Defendant seeks summary judgment as to Plaintiffs' breach of contract claim (Count One) and declaratory judgment claim (Count Two). (See Docs. 1, 8, 9).
- ² The Court addresses whether Plaintiff CTKS suffered a single loss or several distinct losses in Part IV.A, *infra*.
- ³ See Docs. 12, 14-1.
- ⁴ See Docs. 13, 15-1.
- ⁵ Plaintiffs admit that this paragraph describes one of three distinct covered losses claimed by Plaintiffs, the other two being losses due to "not enjoying the benefits of the fraudulent cashier's checks and the failure of the purported Erick Carpenter to pay \$141,750 to plaintiffs as promised." (See Doc. 9 at 17; Doc. 15 at 2, 19-21).
- ⁶ The titles of these forms are capitalized throughout the Policy, and the numbers and letters denoting separate paragraphs, and those paragraph titles, appear in bold text. For ease of reading, the Court will not employ capital letters when referring to the Policy forms (unless part of a quotation) and will not employ bold text when referring to paragraphs within the Policy (even when part of a quotation).

- 7 Plaintiffs admit that this quote is accurate but note that it does not reflect the entire description of "Covered Property" contained in the Policy.
- 8 Plaintiffs admit that \$141,750 was wired from CTKS's IOLTA (trust) account and, thus, lost, but deny this was CTKS's only loss of \$141,750. *See supra* note 5 and accompanying text.
- 9 Plaintiffs admit that the portion of this paragraph in quotation marks is a verbatim quote from "Paragraph A" but note that it does not reflect the entirety of the requirements for coverage under the Policy.
- 10 Plaintiffs admit that the portion of this paragraph in quotation marks is a verbatim quote from pages 3–4 of 39 of the Policy but note that it does not reflect the entirety of the requirements for coverage of losses under the Policy.
- 11 Plaintiffs admit that the portion of this paragraph in quotation marks is a verbatim quote of the language found on page 25 of 39 of the Policy (except for the inserted word "or") but note that does not reflect the entirety of the language found on that or the previous page of the Policy.
- 12 Assuming that this paragraph refers to the "exclusions" in Paragraph 20, Plaintiffs admit this fact.
- 13 The Court will employ these provision titles as shorthand to refer to the relevant policy language. The Business Personal Property and the Business Income and Extra Expense provisions are located in the Businessowners' Property Coverage Special Form. For relevant policy language, see Part IV.C, *infra*. The Computer Fraud coverage extension is located in the Lawyer's Endorsement. For relevant policy language, see Part II.B at ¶ 19, *supra*.
- 14 While Plaintiffs do not explicitly state that Ohio law governs interpretation questions raised in these motions, they cite Ohio law for the breach of contract standard (see Doc. 9 at 18) and cite to Ohio law for contract interpretation principles in their memoranda (see, e.g., Doc. 19 at 9). As Defendant notes, the Policy was issued by Defendant to Plaintiff CTKS, an Ohio insured, in Ohio.
- 15 Regarding the First Loss, the cashier's checks Plaintiffs received from North American were fraudulent. *See supra* Part II.A at ¶ 20, 21. Regarding the Second Loss, Plaintiff CTKS wired \$141,750 to the Japanese bank account of the person purporting to be Erick Carpenter. *See supra* Part II.A at ¶ 19. Regarding the Third Loss, the person purporting to be Erick Carpenter informed Plaintiff Schmidt that he would send a check for \$141,750, but Plaintiffs never received such a check. *See supra* Part II.A at ¶ 22, 23.
- 16 Under the policy in at issue in *Martin*, "Covered Causes of Loss include 'risks of direct physical loss,' but exclude 'loss or damage caused by or resulting from ... [v]oluntary parting with any property by you or anyone else to whom you have entrusted the property.'" *Martin*, 2014 WL 460045, at *1.
- 17 The court provided the following citation:
See, e.g., *Morris James, LLP v. Cont'l Cas. Co.*, 928 F.Supp.2d 816, 819, 823 (D.Del.2013) (finding that where law firm transferred proceeds of forged check to third-party account on the instruction of purported client, the insured had "voluntarily part[ed]" with the funds despite being induced to do so by fraud); *PNS Jewelry, Inc. v. Penn-Am. Ins. Co.*, No. B212348, 2010 Cal.App. Unpub. LEXIS 1467, 2010 WL 685967, at *4 (Cal.Ct.App. Mar. 1, 2010) ("The word 'voluntary' applies to the insured's 'parting' with the property—i.e., when the insured purposely parts with the property without force.... Although the owner was tricked into doing so ..., the owner physically and purposely handed over the property...."); *LaPerla, Ltd. v. Peerless Ins. Co.*, 51 Conn.Supp. 241, 980 A.2d 971, 971–83 (Conn.Super.Ct.2009) (holding that sale of jewelry to fraudster who presented bad check fell within **exclusion** for losses resulting from "[v]oluntary parting with any property by you or anyone entrusted with property if induced to do so by any fraudulent scheme, trick, device or false pretense"); see also Mem. at 6–7, 7 n. 2 (collecting cases); cf. 3 WAYNE R. LAFAYE, SUBSTANTIVE CRIMINAL LAW § 19.7 (2d ed. 2013) ("[T]he crime of false pretenses requires that the defendant ... obtain title to the victim's property.... Whether title to property delivered to the defendant passes to him usually depends upon whether the victim *intends* to transfer title to him....").
Martin, 2014 WL 460045, at *3 (footnote omitted).
- 18 The Court notes that the cases cited by the *Martin* court and by Defendant in its memoranda address provisions that specifically exclude **voluntary partings** induced by fraud or trick. See, e.g., *Morris James, LLP v. Cont'l Cas. Co.*, 928 F.Supp.2d 816; *PNS Jewelry, Inc.*, 2010 WL 685967. However, as the court in *Martin* helpfully explains: "the **Voluntary Parting Exclusion** applies to *any* **voluntary parting** with property. Therefore, it is *broad*er than **exclusions** with additional language limiting the **exclusion** to only **voluntary partings** induced by fraud, scheme, or trick." *Martin*, 2014

WL 460045, at *4 (emphasis in original).

- 19 See *Cook v. Home Depot U.S.A., Inc.*, No. 2:06-cv-00571, 2007 WL 710220, at *9 (S.D.Ohio Mar. 6, 2007); *Scott v. Fairbanks Capital Corp.*, 284 F.Supp.2d 880, 894 (S.D.Ohio 2003); *State ex rel. Dickman v. Defenbacher*, 151 Ohio St. 391, 395, 86 N.E.2d 5 (1949); *Vindicator Printing Co. v. State*, 68 Ohio St. 362, 370, 67 N.E. 733 (1903); *Nationwide Life Ins. Co. v. Myers*, 67 Ohio App.2d 98, 103, 425 N.E.2d 952 (1980); see also 70 C.J.S. Payment § 107 (2005) ("A voluntary payment, within the meaning of the rule that such a payment cannot be recovered, means a payment made by a person of his own motion, without compulsion; a payment made without a mistake of fact or fraud, duress, coercion, or extortion, on a demand which is not enforceable against the payor; and whether in a given case a payment is voluntary depends on the facts of the particular case, as indicating an intention on the part of the payor to waive his legal rights.").
- 20 Plaintiffs also argue that, because Plaintiff Schmidt was required to promptly deliver the funds to his client, the purported Erick Carpenter, any voluntariness on Plaintiff Schmidt's part was eliminated. See Ohio Rule of Professional Conduct 1.15(d) ("Except as stated in this rule or otherwise permitted by law or by agreement with the client or a third person, confirmed in writing, a lawyer shall promptly deliver to the client or third person any funds or property that the client or third person is entitled to receive.") (emphasis omitted); see also 70 C.J.S. Payment § 107 (2005) ("A voluntary payment, within the meaning of the rule that such a payment cannot be recovered, means a payment made by a person of his own motion, without compulsion"); *United Nat'l Ins. Co. v. SST Fitness Corp.*, 309 F.3d 914, 923 (6th Cir.2002) (insurer was not a volunteer because the insured requested the insurer's payment, the insurer asserted a claim in contract and not in equity, and the insurer reserved its right to recoupment). Again, the treatise and case cited address whether a payor can recoup his payment, not whether the payor voluntarily parted with funds.
- 21 In their reply memorandum, Plaintiffs argue that the Computer Fraud coverage extension covers Plaintiff's Second Loss, so, at worst, there is a conflict between the language of the Computer Fraud coverage extension and the "voluntary parting" exclusion, resulting in an ambiguity that must be resolved in Plaintiffs' favor. See *Morris James LLP*, 928 F.Supp.2d 816. In *Morris James*, there was some question as to whether the relevant exclusionary language prevailed over the relevant coverage provision, and the court found that an ambiguity existed between the coverage afforded to losses that resulted from a forged instrument and the exclusion of losses resulting from a voluntary parting induced by fraud. Here, the Lawyers Endorsement (which contains the Computer Fraud provision) "modifies insurance provided under" the Businessowners Property Coverage Special Form. (Doc. 8-2 at 42, 45). The exclusionary language is found in that form, which explicitly states "[w]e will not pay for loss or damage caused by or resulting from ... [v]oluntary parting with any property by you or anyone else to whom you have entrusted the property." (*Id.* at 25-26). It is undisputed that the Lawyers Endorsement does not provide that the "voluntary parting" exclusion is inapplicable to the Computer Fraud coverage extension. See *supra* Part II.B at ¶ 21. Further, the Computer Fraud coverage extension affirmatively states that Paragraph B.2.o. (which contains an exclusion for the transfer of property to a person or place outside the described premises on the basis of unauthorized instructions) does not apply to the coverage extension. (Doc. 8-2 at 45). Logic suggests, then, that the other exclusions contained in the Businessowners Property Coverage Special Form do apply. For this reason, the Court declines to find the ambiguity Plaintiffs suggest.
- 22 The "described premises" are CTKS' law offices at 250 E. 5th Street, Suite 1200, Cincinnati, Ohio. (Doc. 8-2 at 1).
- 23 In *Florists' Mut. Ins. Co. v. Ludy Greenhouse Mfg. Corp.*, 521 F.Supp.2d 661, 680 (S.D.Ohio 2007), the court found that a basic requirement for coverage under Florists' legal liability coverage form was that the insured sustain a loss as a result of "direct physical loss or damage". The Court held that "funds deposited into a bank account do not have a 'physical' existence and, thus, are not susceptible to physical loss or damage." *Id.* Plaintiffs try to distinguish *Florists' Mutual* on the grounds that, unlike funds deposited in a bank, a security in the form of a cashier's check has a physical existence and Plaintiffs' loss of the checks' benefits was directly related to the checks' physical nature (as fakes). Put another way, Plaintiffs argue that because of the cashier's checks' physical characteristics, they were not treated as representations of money, as each purported to be. While the loss may be attributable to the purported checks' physical characteristics, these "checks" and never had any value in the first instance and, in any event, were unchanged upon receipt by Plaintiffs. The purported checks were not physically lost or damaged, as required by the plain language of the Policy.
- 24 The "described premises" are CTKS' law offices at 250 E. 5th Street, Suite 1200, Cincinnati, Ohio. (Doc. 8-2 at 1).
- 25 See Part IV.C.1, *supra* (finding that Plaintiffs have not presented evidence of direct physical loss of or damage to property).

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.

2017 WL 3278060

Only the Westlaw citation is currently available.
United States District Court,
S.D. Texas, Houston Division.

SPEC'S FAMILY PARTNERS, LTD., Plaintiff,

v.

THE HANOVER **INSURANCE** COMPANY, Defendant.

CIVIL ACTION H-16-438

|

Filed in TXSD on 03/15/2017

MEMORANDUM OPINION & ORDER

Gray H. Miller United States District Judge

*1 Pending before this court is defendant Hanover **Insurance** Company's ("Hanover") (1) motion for judgment on the pleadings (Dkt. 19), (2) request for judicial notice in support of its motion (Dkt. 20), and (3) motion for leave to file supplemental authority in support of its motion (Dkt. 30). Also pending before the court is plaintiff Spec's Family Partners, Ltd. (Spec's) motion for leave to file supplemental authority (Dkt. 35). Upon consideration of the pleadings, motion, response, reply, and applicable law, Hanover's motion is GRANTED. Dkt. 19. Further, Hanover's request for judicial notice (Dkt. 20), Hanover's motion for leave to file supplemental authority (Dkt. 30), and Spec's motion for leave to file supplemental authority (Dkt. 35) are DISMISSED AS MOOT.

I. BACKGROUND

This case is about an **insurance** claim made by plaintiff Spec's Family Partners, Ltd. ("Spec's") following two **data breaches** of its credit card payment system. Dkt. 6 at 2. Spec's is a family-owned retail chain. *Id.* Hanover issued an **insurance** policy to Spec's for the period between October 28, 2013 to October 28, 2014 (the "Policy"). Dkt. 19, Ex. A (Policy No. LHD 8930093 03).

Between October 2012 and February 2014, Spec's credit card payment system suffered from two **data breaches**, resulting in the loss of customer information and credit card numbers. Dkt. 6 at 2. Spec's accepts payments from customers using Visa or MasterCard through a third-party transaction service provided by First Data Merchant Services, LLC ("FirstData"). *Id.* In 2001, Spec's entered into a contract with EFS National Bank for credit card transaction services (the "Merchant Agreement"). *Id.*; Dkt. 19, Ex. B. FirstData is the successor to EFS National Bank in the Merchant Agreement. Dkt. 6 at 2. FirstData sent two demand letters to Spec's for claims arising from the **data breaches**: (1) a December 16, 2013 demand letter for \$7,624,846.21 and (2) a March 25, 2015 demand letter for \$1,978,019.49. Dkt. 19, Exs. C, D (collectively "the Underlying Claim"). The letters also demanded that Spec's upgrade its security. *Id.* To satisfy its demands, FirstData incrementally withheld an alleged \$4.2 million from Spec's daily payment card settlements, placing the funds in a reserve account. Dkt. 6 at 2-3.

On April 8, 2014, Spec's notified Hanover of FirstData's December 16, 2013 demand letter. *Id.*; Dkt. 19 at 11. Hanover and Spec's engaged in a series of exchanges regarding Hanover's duty to defend. *Id.* Ultimately, on November 5, 2014, Hanover and Spec's entered into a Defense Funding Agreement ("DFA") in which Hanover consented to the retention

of Haynes and Boone, LLP as defense counsel in litigation regarding the Underlying Claim. Dkt. 24, Ex. D. On April 1, 2015, Spec's notified Hanover of FirstData's March 25, 2015 demand letter. Dkt. 6 at 2–3.

Then, Spec's initiated a lawsuit in United States District Court for the Western District of Tennessee asserting breach of contract claims against FirstData to recover the money it withheld from Spec's (the "Tennessee Litigation"). Dkt. 6 at 3–4. Hanover eventually refused to pay the litigation expenses for the Tennessee Litigation. *Id.*

*2 On March 11, 2016, Spec's filed an amended complaint against Hanover, asserting causes of action for breach of the Policy and breach of the DFA. Dkt. 6 at 5–6. Spec's seeks declaratory judgment on Hanover's duty to defend, damages under Chapter 542 of the Texas Insurance Code, and attorneys' fees. *Id.* at 6–7. Subsequently, Hanover moved for judgment on the pleadings. Dkt. 19. In support of its motion, Hanover has requested the court take judicial notice of the Merchant Agreement and the filings in the Tennessee Litigation. Dkt. 20. Later, both Hanover and Spec's moved to file supplemental authority in support of their pleadings. Dkts. 30, 35. Spec's responded to both of Hanover's motions (Dkts. 23, 25, 31) and Hanover replied (Dkts. 28, 29, 37); Hanover also responded to Spec's motion (Dkt. 36).

II. LEGAL STANDARD

A. Motion for Judgment on the Pleadings

A motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c) is "[d]esigned to dispose of cases where the material facts are not in dispute and a judgment on the merits can be rendered by looking to the substance of the pleadings and any judicially noticed facts." *Great Plains Tr. Co. v. Morgan Stanley Dean Witter & Co.*, 313 F.3d 305, 312 (5th Cir. 2002). Federal Rule of Civil Procedure 12(c) allows a party to move for judgment on the pleadings after the pleadings are closed, as long as it is early enough not to delay trial. Fed. R. Civ. P. 12(c). The standards for a Rule 12(c) motion for judgment on the pleadings and a 12(b)(6) motion to dismiss are the same. *Gentilello v. Rege*, 627 F.3d 540, 543–44 (5th Cir. 2010).

Rule 12(b)(6) allows dismissal if a plaintiff fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). Additionally, the Supreme Court has confirmed that Rule 12(b)(6) motions must be read in conjunction with Rule 8(a), which requires "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a); *Ashcroft v. Iqbal*, 556 U.S. 662, 129 S. Ct. 1937 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 555, 127 S. Ct. 1955 (2007). In considering a Rule 12(b)(6) motion to dismiss a complaint, courts generally must accept the factual allegations contained in the complaint as true. *Kaiser Aluminum & Chem. Sales, Inc. v. Avondale Shipyards, Inc.*, 677 F.2d 1045, 1050 (5th Cir. 1982). The court does not look beyond the face of the pleadings in determining whether the plaintiff has stated a claim under Rule 12(b)(6). *Spivey v. Robertson*, 197 F.3d 772, 774 (5th Cir. 1999). "[A] complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, [but] a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555 (citations omitted). And, "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Id.* The supporting facts must be plausible—enough to raise a reasonable expectation that discovery will reveal further supporting evidence. *Id.* at 556.

A court considers only the pleadings in deciding a motion for judgment on the pleadings, but "[d]ocuments that a defendant attaches to a motion to dismiss are considered part of the pleadings if they are referred to in the plaintiff's complaint and are central to her claim." *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498–99 (5th Cir. 2000). Because the standards for Rule 12(c) and 12(b)(6) motions are the same, a court may consider the same kind of documents in a Rule 12(c) motion that it could consider in a Rule 12(b)(6) motion. See *Horsley v. Feldt*, 304 F.3d 1125, 1134 (11th Cir. 2002) (permitting the consideration of additional documents in a motion for judgment on the pleadings).

B. Duty to Defend

*3 Under Texas law, courts follow the “eight corners rule” to determine whether an insurer has a duty to defend. *Federated Mut. Ins. Co. v. Grapevine Excavation Inc.*, 197 F.3d 720, 723 (5th Cir. 1999). “Under this rule, courts compare the words of the insurance policy with the allegations of the plaintiff's complaint to determine whether *any* claim asserted in the pleading is potentially within the policy's coverage.” *Id.* “The duty to defend analysis is not influenced by facts ascertained before the suit, developed in the process of litigation, or by the ultimate outcome of the suit.” *Primrose Operating Co. v. Nat'l Am. Ins. Co.*, 382 F.3d 546, 552 (5th Cir. 2004). Rather, it is determined by examining the eight corners of the pleadings and the policy. *Zurich Am. Ins. Co. v. Nokia, Inc.*, 268 S.W.3d 487, 491 (Tex. 2008). All doubts with regard to the duty to defend are resolved in favor of the duty. *Id.* Courts applying the eight corners rule “give the allegations in the petition a liberal interpretation.” *Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Merchants Fast Motor Lines, Inc.*, 939 S.W.2d 139, 141 (Tex. 1997). Courts must not, however, “read facts into the pleadings, ... look outside the pleadings, or imagine factual scenarios which might trigger coverage.” *Id.* at 142.

The insured has the burden of showing that a claim is potentially within the coverage of the policy. *Federated Mut. Ins. Co.*, 197 F.3d at 723. However, “if the insurer relies on the policy's exclusions, it bears the burden of proving that one or more of those exclusions apply. ... Once the insurer proves that an exclusion applies, the burden shifts back to the insured to show that the claim falls within an exception to the exclusion.” *Id.* Courts “must adopt the construction of an exclusionary clause urged by the insured as long as that construction is not itself unreasonable, even if the construction urged by the insurer appears to be more reasonable or a more accurate reflection of the parties' intent.” *Barnett v. Aetna Life Ins. Co.*, 723 S.W.2d 623, 666 (Tex. 1987). However, the “rules favoring the insured ... are applicable only when there is an ambiguity in the policy; if the exclusions in question are susceptible to only one reasonable construction, these rules do not apply.” *Canutillo Indep. Sch. Dist. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 99 F.3d 695, 701 (5th Cir. 1996).

III. ANALYSIS

First, the court will consider the nature of the Underlying Claim and whether Hanover has a duty to defend Spec's. Dkt. 6, 19. As part of the duty to defend analysis, the court will address Spec's causes of action for breach of Policy and breach of the DFA. Dkt. 6. Then, the court will consider if a cause of action arises from a breach of the duty to defend under the Texas Insurance Code. Dkts. 6, 19. Finally, the court will address Hanover's request for a declaratory judgment on the duty to indemnify (Dkt. 19), Hanover's request for judicial notice (Dkt. 20) and Hanover and Spec's motions for leave to supplement the pleadings (Dkt. 30, 35).

A. The Underlying Claim

As an initial matter, the court will clarify the nature of the Claim at issue in this case to define the scope of the duty to defend analysis.

The Policy contains the following relevant provisions:

1. Defense of Claims:

We have the right and duty to defend “Claim,” even if the allegations in such “Claims” are groundless, false or fraudulent. We have no duty to defend “Claims” or pay related “Defense Expenses” for “Claims to which this insurance does not apply.”

Dkt. 19, Ex. A at HJOP 0014.

2. Definition of Claim

[A] "Claim" means: (1) Any written demand presented for monetary "Damages" or non-monetary relief for a "Wrongful Act"; or (2) Any complaint or similar pleading initiating a judicial, civil, administrative, regulatory, alternative dispute, or arbitration proceeding, including any appeal resulting from it, to which an "Insured" is provided notice and which subjects an "Insured" to a binding adjudication of liability for monetary or non-monetary relief for a "Wrongful Act"

*4 Dkt. 19, Ex. A at HJOP 0025–26.

Spec's offers two items that qualify as "written demand[s] presented for monetary 'Damages' or non-monetary relief" under the definition of a "Claim" in the policy—the two demand letters from FirstData to Spec's for "indemnification" of monetary damages and security upgrades. Dkt. 19, Exs. C (December 16, 2013 demand letter), D (March 25, 2015 demand letter). The court concludes these two demand letters fall under the definition of a "Claim" as defined in the Policy. Dkt. 23 at 16.

However, both Hanover and Spec's argue for a more inclusive definition of a claim beyond these two demand letters: (1) Spec's alleges that the fines from MasterCard and Visa are part of the claim, and (2) Hanover argues that the claim is actually the Tennessee Litigation, which presents no claim to defend. Dkt. 23 at 19; Dkt. 28 at 3.

First, Spec's asserts that fines from MasterCard and Visa, as well as the administrative process to dispute those fines, are part of the Underlying Claim. Dkt. 23 at 19. Though the two demand letters detail fines owed or potentially owed to MasterCard and Visa, the demand letters are not from either MasterCard or Visa, they are from FirstData. *Id.* In FirstData's December 16, 2013 demand letter, the letter concludes that "... in accordance with Spec's indemnification obligation in the EFS National Bank Merchant Agreement ... First Data Merchant Services Corporation will be establishing a Reserve Account ... to fund the MasterCard and the anticipated Visa fines." Dkt. 19, Ex. C. The letter provides no other grounds for FirstData's collection of these fines beyond the Merchant Agreement. *Id.* In FirstData's March 25, 2015 demand letter, FirstData also concludes the letter by stating that it is establishing a reserve account to collect the fines "in accordance with Spec's various contractual obligations." Dkt. 19, Ex. D.

Based on these statements, taken with the content of the letters, the court concludes that the MasterCard and Visa fines are levied against FirstData. The details of the fines in the demand letters are provided as the basis for the amount demanded by FirstData under the indemnification obligation of the Merchant Agreement. These fines from MasterCard and Visa do not represent a separate demand against Spec's and so they are not a "claim" by the definition in the Policy.

Second, Hanover makes a collateral attack in its reply that there is no underlying petition at all, and therefore the eight corners rule does not apply to this case. Dkt. 28 at 3. If the only claim at issue is the Tennessee Litigation, in which Spec's is the plaintiff, there is no claim under the definition of the Policy that gives rise to the duty to defend. Dkt. 28 at 3 (citing to *Agilis Ben. Servs. LLC v. Travelers Cas. & Sur. Co. of Am.*, No. 5:08-CV-213, 2010 WL 8573372, at *2 (E.D. Tex. Apr. 30, 2010) and *SMBC Rail Servs., LLC v. W. Petroleum Co.*, No. 3:14-CV-03982-P, 2015 WL 7709608, at *3 (N.D. Tex. June 17, 2015)). Hanover's argument in its reply appears to ignore the existence of the two demand letters, which form the Underlying Claim. Dkt. 19, Exs. C, D. The court rejects any argument that there is no underlying claim and concludes the eight corners rule is applicable to the duty to defend analysis. The court will consider the four corners of the demand letters and the four corners of the Policy. Dkt. 19, Exs. A, C, D.

*5 Spec's also counters that Hanover is improperly trying to raise the merits of the Underlying Claim by presenting details of the Tennessee Litigation outside of the eight corners rule. Dkt. 23 at 28. "Facts ascertained before suit, developed in the process of litigation, or determined by the ultimate outcome of the suit do not affect the duty to defend." *Northfield Ins. Co. v. Loving Home Care, Inc.*, 363 F.3d 523, 528 (5th Cir. 2004) (citing *Trinity Universal Ins. Co. v. Cowan*, 945 S.W.2d 819, 829 (Tex. 1997)). The eight corners rule prevents the court from considering the merits and nature of the Tennessee Litigation in determining whether Hanover has a duty to defend.

B. Duty to Defend Analysis

The court turns to the central issue of whether Hanover has a duty to defend Spec's against FirstData's demands. Hanover argues that the only claim Spec's asserted is FirstData's demand for indemnification based on the Merchant Agreement—which is expressly excluded from Policy coverage. Dkt. 19 at 14–15. The Policy contains the following exclusion which precludes claims based upon a written contract:

N. 'Loss' on account of any 'Claim' made against any 'Insured' directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. However, this exclusion does not apply to your liability that would have attached in the absence of such contract or agreement.

Dkt. 19, Ex. A at HJOP 0029 ("Exclusion N").

Hanover bears the burden of proof to demonstrate the applicability of the policy exclusion. *Federated Mut. Ins. Co.*, 197 F.3d at 723. Both demand letters stated that FirstData's claims against Spec's are asserted in accordance with Spec's indemnification obligation under the Merchant Agreement, so Hanover argues this is proof that it is a clearly excluded claim under Exclusion N. Dkt. 19 at 14–15. The court will consider Spec's arguments that Exclusion N does not apply because (1) Hanover agreed to defend Spec's, (2) there is a potential for claims that are not barred by Exclusion N, and (3) this case arises out of underlying criminal activity.

1. Hanover's alleged agreement to defend Spec's

First, Spec's argues that Exclusion N is inapplicable because Hanover already agreed to defend Spec's against FirstData. Dkt. 23 at 8; Dkt. 24, Ex. C (August 22, 2014 message). Hanover counters that in any agreements it made with Spec's, it properly reserved its rights to challenge its duty to defend or withdraw its defense. Dkt. 28 at 2–3. Normally, in a duty to defend suit, the court does not consider extrinsic evidence that is outside of the limits of the eight corners rule, which only allows the court to consider the petition in the Underlying Claim and the Policy. *Federated Mut. Ins. Co.*, 197 F.3d at 723. However, the court will review evidence of Hanover's agreements with Spec's for the limited purposes of determining whether Hanover's representations modified the Policy. Dkt. 24, Exs. C (August 22, 2014 message), D (DFA).

First, in its August 22, 2014 message to Spec's, Hanover stated it "agrees to withdraw its denial of coverage and provide a defense under a reservation of rights as set forth below." Dkt. 24, Ex. C at 17. However, in reviewing Hanover's message, the court finds that Hanover reserved its rights to challenge its duty to defend or to withdraw its defense by stating:

Please be advised that ... nothing contained herein, nor any action nor inaction on the part of Hanover or any agent or representative thereof, should be construed as a waiver of any [of] Hanover's rights, privileges, and defenses under the Policy, included but not limited to ... any rights and defenses available at law or in equity to deny coverage in the event that any terms, conditions, exclusions and endorsements ... are found to be applicable, including the right to withdraw from the defense ...

*6 *Id.* at 27.

Further, Spec's alleges that Hanover also consented to defense by executing the DFA. Dkt. 23 at 13–14; Dkt. 24, Ex. D. The DFA states "Hanover has agreed to defend the claim ... subject to a reservation of rights ..." Dkt. 24, Ex. D at 28. The DFA also states that "the Parties disagree regarding the effect of Hanover's reservation of rights on its right and duty to defend the Claim under the Policy." *Id.* Finally the DFA states that "Hanover consents to the continued retention of Haynes and Boone as defense counsel and will pay, subject to its reservation of rights" Dkt. 24, Ex. D at 28.

"A reservation of rights is a proper action if the insurer believes, in good faith, that the complaint alleges conduct which may not be covered by the policy." *Rhodes v. Chicago Ins. Co., a Div. of Interstate Nat. Corp.*, 719 F.2d 116, 120 (5th Cir. 1983); *see also Tex. Ass'n Gov't Risk Mgmt. Pool v. Matagorda County*, 52 S.W.3d 128, 132-33 (Tex. 2000). Under Texas law, an insurer can undertake a defense subject to a reservation of rights, which "permit the insurer to provide a defense for its insured while it investigates questionable coverage issues." *Canal Ins. Co. v. Flores*, 524 F. Supp. 2d 828, 834 (W.D. Tex. 2007) (citing to *Katerndahl v. State Farm Fire & Cas. Co.*, 961 S.W.2d 518, 521 (Tex. App.—San Antonio 1998, no pet.)); *see also Certain Underwriters at Lloyd's London v. A & D Interests, Inc.*, 197 F. Supp. 2d 741, 745 (S.D. Tex. 2002). Under a valid reservation of rights, the insurer may withdraw its defense when it is clear there is no coverage under its policy. *Id.*; *see also Ross v. Marshall*, 456 F.3d 442, 443 (5th Cir. 2006) ("An insurer who defends its insured under a full reservation of rights provides a defense in the liability action, but reserves the right to contest coverage later.") (citing to *Arkwright-Boston Mfrs. Mut. Ins. Co. v. Aries Marine Corp.*, 932 F.2d 442, 445 (5th Cir. 1991)).

Here, Hanover properly reserved its rights in the August 22, 2014 message. Dkt. 24, Ex. C. The DFA directly addresses the issue of the disagreements over the meaning of the Agreement and includes the provision: "Except as may be stated herein, no part of this Agreement shall constitute a waiver, release or relinquishment of any of the Parties' respective rights, obligations, claims or defenses under the Policy, nor shall this Agreement constitute an admission by either party of any disputed matter between them." Dkt. 24, Ex. D at 29. The express terms of the DFA contradict Spec's assertion that the DFA functions as an "admission" of Hanover's duty to defend and a waiver of its rights under the Policy. *Id.* The court finds that August 22, 2014 message and the DFA expressly reserve Hanover's rights, and neither serve to modify the Policy or act as a waiver to Exclusion N. Therefore, Spec's is not entitled to a defense by the terms of the August 22, 2014 message or the DFA. Spec's claim that Hanover breached the DFA is DISMISSED.

2. Potential claims that are not barred by Exclusion N

*7 Second, Spec's argues that the Underlying Claim potentially includes non-contract claims, which are not excluded by the Policy. Dkt. 23 at 17–19. Exclusion N does not apply if liability "would have attached in the absence of such contract or agreement." Dkt. 19, Ex. A. Further, under the eight corners rule, if the petition in the Underlying Claim contains any allegations that do not fall under a policy exclusion, the insurer continues to have a duty to defend. *Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Merchants Fast Motor Lines, Inc.*, 939 S.W.2d 139, 141 (Tex. 1997) ("[I]n case of doubt as to whether or not the allegations of a complaint against the insured state a cause of action within the coverage of a liability policy sufficient to compel the insurer to defend the action, such doubt will be resolved in insured's favor.") (internal citations omitted). But, "[i]f the petition only alleges facts excluded by the policy ... the insurer is not required to defend." *Northfield*, 363 F.3d at 528 (citing *Fid. & Guar. Ins. Underwriters, Inc. v. McManus*, 633 S.W.2d 787, 788 (Tex. 1982)). In evaluating the duty to defend, the court only looks at the alleged facts in the Underlying Claim, not any asserted legal theories. *Id.* (citing *St. Paul Fire & Marine Ins. Co. v. Green Tree Fin. Corp.-Tex.*, 249 F.3d 389, 392 (5th Cir. 2001)).

Here, Spec's argues that the MasterCard and Visa fines and the funding of a reserve account to pay for those fines do not arise out of its contract with FirstData. Dkt. 23 at 19 ("FirstData's own allegations against Spec's do not articulate a contractual basis for liability.") As the court has already discussed, there is no written demand directly from MasterCard and Visa against Spec's, the Underlying Claim is that of FirstData against Spec's. Spec's argues that FirstData does not "suggest any provision of the Merchant Agreement [which] entitles it to 'establish a Reserve Account' and unilaterally withhold funds. ..." Dkt. 23 at 20. The court agrees that FirstData is not specific in referencing the provisions of the Merchant Agreement it is invoking in its demand letters, but FirstData explicitly states that it is demanding "indemnification," which is a contractual obligation that arises from the Merchant Agreement Dkt. 19, Exs. C, D.

"A court may not ... speculate as to factual scenarios that might trigger coverage or create an ambiguity." *Gilbane Bldg. Co. v. Admiral Ins. Co.*, 664 F.3d 589, 596 (5th Cir. 2011). Spec's is asking the court to look beyond FirstData's demand letters, in violation of the eight corners rule, to find a speculative factual scenario or legal theory in which MasterCard or Visa make a claim directly against Spec's. Dkt. 28 at 5. Spec's does not identify what this speculative cause of action

might be or explain how a claim could arise outside of FirstData's identification demands, other than to make conclusory statements that such a claim would include "no contractual liability." Dkt. 23 at 19–20. Though the court construes **coverage** liberally and policy exclusions narrowly, the court is not required to imagine a legal theory for a potential claim from a third party who has not even sent a demand letter or filed a petition. *Northfield*, 363 F.3d at 528. The claim at issue here is FirstData's demand letters, which are based only in contractual indemnification.

3. Underlying criminal causation

Third, Spec's argues the Underlying Claim arises out of superceding criminal conduct, the **data breach**, which was the "but for" cause of the claim. Dkt. 23 at 24. Spec's argues that because the criminal activity is an independent cause of the claim, Exclusion N does not apply. Dkt. 23 at 24. In support, Spec's reference cases where an independent cause of action gives rise to claims that also arise from excluded causes. *See, e.g. Utica*, 141 S.W.3d at 204 (affirming a duty to defend based on an injury allegedly caused concurrently by **covered** and excluded events). Hanover counters that the appropriate standard to use is the "incidental relationship" standard rather than "but for" causation. Dkt. 28 at 4 ("[a] claim need only bear an incidental relationship to the described conduct for the exclusion to apply") (quoting *Scottsdale Ins. Co. v. Texas Sec. Concepts and Investigation*, 173 F.3d 941 (5th Cir.1999)).

*8 Again, Spec's is making the argument that there is "potential" for liability that is not precluded by Exclusion N and urges the court avoid construing Exclusion N too broadly. *Id.* at 25. But, the court applies the eight corners rule to look at the policy and the Underlying Claim, and finds that the only claim being made here is by FirstData for indemnification under a contract. Dkts. 19, Ex. C, D. There is nothing in FirstData's demand letter to suggest that it is attempting to recover damages based on a criminal liability theory. Dkt. 28 at 5. That criminal conduct gave rise to this contract claim does not change the basic nature of FirstData's claim against Spec's for contractual liability. This is not the case of a criminal claim that exists independently as Spec's argues—this is just a contractual claim. Spec's fails to allege any facts that show it would be liable or have any form of privity or obligation to pay damages to FirstData for any other reason that those that arise out of contractual liability.

The court finds that Spec's arguments do not assert any ambiguity in the applicability of Exclusion N. The Underlying Claim is based on the Merchant Agreement, and **coverage** of contract claims is clearly excluded by the Policy. Therefore, the court concludes Hanover has no duty to defend the Underlying Claim. Spec's claim against Hanover for breach of the Policy is DISMISSED.

C. **Insurance** Code claims

Spec's also alleges that Hanover is liable under Chapter 542 of the Texas **Insurance** Code by failing to promptly pay for defense expenses incurred. Dkt. 6 at 6; Tex. Ins. Code Ann. §§ 542.058, 542.060. The liability "does not apply in a case in which it is found as a result of ... litigation that a claim received by an insurer is invalid and should not be paid by the insurer." § 542.058(b). Because the court has concluded that Hanover does not have the duty to defend Spec's in the Underlying Claim, Hanover does not owe defense expenses under the Texas **Insurance** Code. Therefore, Spec's claim under the Texas **Insurance** Code is DISMISSED.

D. Duty to Indemnify

Hanover requests a declaratory judgment that Hanover does not have a duty to indemnify because the court finds Hanover lacks a duty to defend. Dkt. 19 at 21; Dkt. 28 at 6. In Texas, an "insurer's duty to defend and duty to indemnify are distinct and separate duties." *Farmers Tex. Cty. Mut. Ins. Co. v. Griffin*, 955 S.W.2d 81, 82 (Tex. 1997). An "insurer may have a duty to defend but, eventually, no duty to indemnify." *Id.* A duty to indemnify may be adjudicated even before the underlying suit proceeds to judgment. *Id.* Here, Spec's complaint does not seek a declaratory judgment on Hanover's duty to indemnify. Dkt. 6 at 7–8. Hanover did not move for a declaratory judgment on the duty to indemnify, but rather raised the issue in its motion for judgment on the pleadings, so Hanover has not properly raised the issue.

Dkt. 19 at 21; Dkt. 28 at 6. Therefore, the court will not consider the merits of a declaratory judgment on the duty to indemnify. Dkt. 23 at 32.

E. Request for Judicial Notice and Motions for Supplemental Authority

Hanover seeks to supplement the record with (1) a request that the court take judicial notice of filings in the Tennessee litigation and the Merchant Agreement and (2) a motion to file supplemental authority. Dkts. 20, 30. Spec's responded and Hanover replied to both of these motions. Dkts. 25, 29, 31, 37. Spec's also moved for leave to file supplemental authority, and Hanover responded. Dkts. 35, 36.

First, Spec's objects to use of extrinsic evidence from the Merchant Agreement and the Tennessee Litigation as because they are not admissible under the eight corners rule.¹ Dkt. 19, Ex. B (the Merchant Agreement) and Dkt. 24, Ex. 1–4 (Tennessee Litigation documents). “Resort[ing] to evidence outside the four corners of [the underlying petition and the insurance policy] is generally prohibited.” *GuideOne Elite Ins. Co. v. Fielder Rd. Baptist Church*, 197 S.W.3d 305, 307 (Tex. 2006). The court can review extrinsic evidence as a narrow exception to the eight corners rule only “when it is initially impossible to discern whether coverage is potentially implicated and when the extrinsic evidence goes solely to a fundamental issue of coverage which does not overlap with the merits of or engage the truth or falsity of any facts alleged in the underlying case.” *Evanston Ins. Co. v. Lapolla Indus., Inc.*, 634 F. App'x 439, 444 (5th Cir. 2015) (internal quotations omitted). The court did not need to apply this narrow exception and use the Merchant Agreement or any of the Tennessee Litigation documents to determine the duty to defend issue.

*9 With regard to the supplemental authority, Spec's seeks to introduce a case out of the Eighth Circuit, which does not offer binding precedent for this court to follow. Dkt. 35 (offering *State Bank of Bellingham v. BancInsure, Inc.*, 2016 WL 2943161 (8th Cir. May 20, 2016)). Likewise, Hanover seeks to introduce a case out of the District of Arizona, which does not offer binding precedent for this court to follow. Dkt. 30 (offering *P.F. Chang's China Bistro Inc. v. Federal Insurance Co.*, 2016 U.S. Dist. LEXIS 70749 (D. AZ. May 31, 2016)). Moreover, the court in its ruling has not relied on the material offered in any of these motions. Therefore Hanover's request for judicial notice, Hanover's motion for leave to file supplemental authority, and Spec's motion for leave to file supplemental authority are DISMISSED AS MOOT. Dkts. 20, 30, 35.

IV. CONCLUSION

Hanover's motion for judgment on the pleadings (Dkt. 19) is GRANTED. Hanover's request for judicial notice (Dkt. 20), Hanover's motion for leave to file supplemental authority (Dkt. 30), and Spec's motion for leave to file supplemental authority (Dkt. 35) are DISMISSED AS MOOT. Spec's claims are DISMISSED WITH PREJUDICE.

The parties are directed to notify the court within seven (7) days if they wish to have this Memorandum Opinion & Order remain sealed.

All Citations

Slip Copy, 2017 WL 3278060

Footnotes

- ¹ The court notes there may be some confusion regarding Spec's response in objection to the motion for judicial notice because of offset exhibit numbering. The Merchant Agreement is attached twice, as Dkt. 19, Ex. B and Dkt. 20, Ex. 1. Tennessee Litigation documents are attached twice as Dkt. 19, Exs. 1–4 and Dkt. 20, Exs. 2–5. It appears that Spec's objected to the

Merchant Agreement twice and failed to object to the last document in the Tennessee Litigation (Dkt. 20, Ex. 5), when Spec's may have intended to object to the full set of Tennessee Litigation documents. Dkt. 25.

End of Document

© 2017 Thomson Reuters. No claim to original U.S. Government Works.

2018 WL 3120794

Only the Westlaw citation is currently available.

This case was not selected for publication in West's Federal Reporter.

See Fed. Rule of Appellate Procedure 32.1 generally governing citation of judicial decisions issued on or after Jan. 1, 2007. See also U.S.Ct. of App. 5th Cir. Rules 28.7 and 47.5.

United States Court of Appeals, Fifth Circuit.

SPEC'S FAMILY PARTNERS, LIMITED, Plaintiff – Appellant Cross-Appellee

v.

THE HANOVER **INSURANCE** COMPANY, Defendant – Appellee Cross-Appellant

No. 17-20263

|
June 25, 2018

Appeals from the United States District Court for the Southern District of Texas

USDC No. 4:16-CV-438

Before KING, JONES, and GRAVES, Circuit Judges.

Opinion

PER CURIAM:*

*1 Spec's Family Partners, Limited sued Hanover **Insurance** Company for refusing to pay its attorney's fees and expenses in defending a claim under the parties' **insurance** policy. Because the district court erred in granting judgment on the pleadings and dismissing all counts of its complaint against Hanover, we REVERSE and REMAND.

I.

A.

Spec's Family Partners, Ltd. ("Spec's") is a specialty retail chain based in Houston that accepts payments from major credit card brands like MasterCard and Visa. To process these credit card payments, in 2001 Spec's entered into a Merchant Agreement with First Data Merchant Services, LLC ("First Data"), a company that processes credit and debit card transactions in exchange for a fee.

Between October 2012 and February 2014, Spec's credit card network was hacked by unknown criminals, which resulted in First Data's having to reimburse issuing banks the costs associated with the fraudulent transactions. First Data demanded payment from Spec's in a letter dated December 16, 2013, claiming there was "conclusive evidence of a breach of the cardholder environment at Spec's," and stating "Spec's was non-compliant with the Payment Card Industry Data Security [Standard] (PCIDSS) requirements." In this first demand letter, First Data listed the prices of the case management fee, fines, and reimbursement costs it used to establish a Reserve Account in the amount of \$7,624,846.21 in order to "fund the Mastercard fines and the anticipated Visa fines." First Data also demanded documentation and security compliance from Spec's, including a completed MasterCard Site Data Protection Account Data Information Form and Attestation of Compliance from a Qualified Security Assessor.

On March 25, 2015, First Data sent a second demand letter to Spec's repeating the same allegations regarding the breach of Spec's cardholder environment. The second demand letter notified Spec's of the establishment of a second Reserve Account in the amount of \$1,978,019.49, comprising the MasterCard fines related to monitoring and replacement costs and fraud reimbursement. Both demand letters established the Reserve Accounts "in accordance with Spec's[]" indemnification obligation" under the Merchant Agreement and stated "nothing contained herein shall be deemed a waiver of any right we may have under the Merchant Agreement or otherwise and we expressly reserve such right." For purposes of this appeal, the parties and the district court treated the December 2013 and March 2015 demand letters as a single "Claim" under the Policy.

B.

In 2013, Hanover issued a Private Company Management Liability **Insurance** Policy (the "Policy") to Spec's for a **coverage** period of October 28, 2013 to October 28, 2014.

The Policy's provision for Directors, Officers and Corporate Liability **Coverage** states:

B. Corporate Entity Liability

We will pay "Loss" which the "Insured Entity" is legally obligated to pay because of "Claims" made against the "Insured Entity" during the "Policy Period" and reported to us during the "Policy Period" for any "Wrongful Act" to which this **insurance** applies.

*2 The Policy defines "Claim" and "Loss" as follows:

A. "Claim" means:

1. Any written demand presented for monetary "Damages" or non-monetary relief for a "Wrongful Act"; or
2. Any complaint or similar pleading initiating a judicial, civil, administrative, regulatory, alternative dispute or arbitration proceeding, including any appeal result from it, to which an "Insured" is provided notice and which subjects an "Insured" to a binding adjudication of liability for monetary or non-monetary relief for a "Wrongful Act."

However, "Claim" shall not include a labor or grievance proceeding pursuant to a collective bargaining agreement.

All "Claims" made on account of a single "Wrongful Act" shall be treated as a single "Claim" made on the date the earliest of the "Claims" was made, regardless of whether that date is before or during the "Policy Period" or, if applicable, during an Extended Reporting Period.

H. "Loss" means the amount the "Insured" is legally obligated to pay for "Damages" and "Defense Expenses" for a **covered** "Claim" under this **Coverage** Part. "Loss" does not include:

1. Any amounts which an "Insured" is obligated to pay as a result of a "Claim" seeking relief or redress in any form other than monetary "Damages;"

The Policy includes the following provision with respect to the defense of "Claims":

VI. DEFENSE OF CLAIMS

We have the right and duty to defend “Claims,” even if the allegations in such “Claims” are groundless, false or fraudulent. We have no duty to defend “Claims” or pay related “Defense Expenses” for “Claims” to which this insurance does not apply....

The Policy also includes a number of exclusions to coverage, including the following provision (“Exclusion N”):

This insurance does not apply to:

N. “Loss” on account of any “Claim” made against any “Insured” directly or indirectly based upon, arising out of, or attributable to any actual or alleged liability under a written or oral contract or agreement. However, this exclusion does not apply to your liability that would have attached in the absence of such contract or agreement.

When Spec’s provided Hanover with timely notice of First Data’s demand letters, Hanover initially refused to defend or indemnify the Claim on the basis it fell within Exclusion N of the Policy by virtue of the Merchant Agreement between Spec’s and First Data. However, on August 22, 2014, Hanover withdrew its denial of coverage and agreed to provide a defense under a reservation of rights. To that end, Hanover and Spec’s entered into a separate Defense Funding Agreement on November 5, 2014, in which Hanover agreed, until such time as it provided written notice to the other party’s identified representatives, to the retention of Haynes and Boone, LLP; promised to pay the firm’s attorneys’ fees at limited hourly rates; and agreed to reimburse Spec’s for defense costs previously incurred in defending the Claim, all “subject to [Hanover’s] reservation of rights.”

To recover the money First Data withheld in the Reserve Accounts, Spec’s filed suit against First Data in the United States District Court for the Western District of Tennessee in December 2014 (the “Tennessee Litigation”).¹ Although Hanover complied with its obligations under the Defense Funding Agreement for a few months, it eventually refused to pay expenses associated with the Tennessee Litigation, claiming they were not “defense expenses” as they were incurred in pursuit of an affirmative claim against First Data. In response, Spec’s brought the claims in this case against Hanover for: (1) breach of the Policy, (2) breach of the Defense Funding Agreement, (3) violation of Chapter 542 of the Texas Insurance Code, and (4) a declaratory judgment that Hanover has an ongoing obligation to pay defense costs.

*3 Hanover moved for judgment on the pleadings under Fed. R. Civ. Pro. 12(c), asserting: (1) Exclusion N of the Policy forecloses “any duty by Hanover to defend or indemnify Spec’s,” and (2) Spec’s is unable to recover “under Chapter 542 of the Texas Insurance Code or Section 38.001 of the Texas Civil Practice and Remedies Code.” The district court granted Hanover’s Rule 12(c) motion and dismissed all of Spec’s claims, finding that while the demand letters were a “Claim” that triggered the duty to defend, Exclusion N precluded coverage because the Claim arose out of the Merchant Agreement between Spec’s and First Data. The district court denied as moot Hanover’s Request for Judicial Notice and Motion to File Supplemental Authority.²

Spec’s timely appealed.

II.

The court reviews a district court’s ruling on a Rule 12(c) motion for judgment on the pleadings *de novo*. *Edionwe v. Bailey*, 860 F.3d 287, 291 (5th Cir. 2017) (citation omitted); *see* Fed. R. Civ. P. 12(c) (“After the pleadings are closed—but early enough not to delay trial—a party may move for judgment on the pleadings.”). A motion for judgment on the pleadings is evaluated using the same standard as a motion to dismiss for failure to state a claim under Rule 12(b)(6). *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008). “[T]he central issue is whether, in the light most favorable to the plaintiff, the complaint states a valid claim for relief.” *Id.* (quoting *Hughes v. Tobacco Inst., Inc.*, 278 F.3d 41, 420

(5th Cir. 2001)). A valid claim for relief is one in which “the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937 (2009). The court accepts “all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff.” *Gines v. D.R. Horton, Inc.*, 699 F.3d 812, 816 (5th Cir. 2012) (internal quotation marks and citation omitted).

III.

Under Texas law, the insured bears the burden of proving a claim against it falls within a policy’s affirmative grant of **coverage**, and the insurer bears the burden of proving an exclusion applies. *Fliess v. State Farm Lloyds*, 392 F.3d 802, 807 (5th Cir. 2004). The primary goal of the court is to give effect to the intention of the parties as expressed in the policy. *Liberty Surplus Ins. Corp. v. Exxon Mobil Corp.*, 483 S.W.3d 96, 100 (Tex. App.—Houston [14th Dist.] 2015, pet. denied). Because ordinary rules of contract interpretation apply to **insurance** contracts, if a court determines the policy is ambiguous, then it must resolve those ambiguities in favor of the insured. *State Farm Fire & Cas. Co. v. Vaughan*, 968 S.W.2d 931, 933 (Tex. 1998). “A policy is unambiguous, as a matter of law, if the court can give it a definite legal meaning.” *Id.*

*4 The Policy in this case involves two different duties: the duty to defend and the duty to indemnify. *See Gilbane Bldg. Co. v. Admiral Ins. Co.*, 664 F.3d 589, 594 (5th Cir. 2011) (citing *D.R. Horton-Tex., Ltd. v. Markel Int’l Ins. Co.*, 300 S.W.3d 740, 743 (Tex. 2009)). These duties are distinct and should generally be decided separately. *See id.* (citing *D.R. Horton*, 300 S.W.3d at 743). Under the eight-corners rule, an insurer’s duty to defend is determined by “the **insurance** policy and the third-party plaintiff’s pleadings in the underlying litigation, which the court must review ‘without regard to the truth or falsity of those allegations.’” *Amerisure Ins. Co. v. Navigators Ins. Co.*, 611 F.3d 299, 309 (5th Cir. 2010) (quoting *GuideOne Elite Ins. Co. v. Fielder Rd. Baptist Church*, 197 S.W.3d 305, 308 (Tex. 2006)). In determining the duty to indemnify, however, the court is not bound by the eight-corners rule but may instead look to the evidence introduced by the parties during the **coverage** litigation. *See D.R. Horton*, 300 S.W.3d at 741. Although “one duty may exist without the other,” *id.* at 743, the same reasons that negate one duty may also negate the other, *see Farmers Tex. Cty. Mut. Ins. Co. v. Griffin*, 955 S.W.2d 81, 84 (Tex. 1997).

Whether Hanover owed Spec’s a duty to defend turns on whether the two demand letters contain at least one claim that potentially falls within Hanover’s scope of **coverage** under the Policy. Again, the duty to defend arises “if at least one of several claims in the plaintiff’s complaint potentially falls within the scope of **coverage**, even if other claims do not.” *Federated Mut. Ins. Co. v. Grapevine Excavation Inc.*, 197 F.3d 720, 726 (5th Cir. 1999). Spec’s and Hanover disagree over whether the statements made by First Data in its demand letters allege an occurrence giving rise to the duty to defend or whether they fall entirely under the type of allegations barred by Exclusion N – namely, losses that directly or indirectly are based upon, arise out of, or are attributable to any actual or alleged liability under a written or oral contract or agreement.

Where an underlying petition includes allegations that “go beyond” conduct **covered** by an exclusion, the duty to defend is still triggered. *Great Am. Ins. Co. v. Calli Homes, Inc.*, 236 F. Supp. 2d 693, 703 (S.D. Tex. 2002). Even “in case of doubt as to whether or not the allegations of a complaint against the insured state a cause of action within the **coverage** of a liability policy sufficient to compel the insurer to defend the action, such doubt will be resolved in [the] insured’s favor.” *Nat’l Union Fire Ins. Co. v. Merchs. Fast Motor Lines, Inc.*, 939 S.W.2d 139, 141 (Tex. 1997) (alteration added) (quoting *Heyden Newport Chem. Corp. v. Southern Gen. Ins. Co.*, 387 S.W.2d 22, 26 (Tex. 1965)). In line with these principles, Hanover’s duty to defend is triggered if the Claim included the potential for liability on a non-contractual ground, even if the Claim may also have asserted contractual liability that would be barred by Exclusion N. Additionally, Exclusion N does not apply to “liability that would have attached in the absence of such contract,” so the possibility that “a claim could arise out of contractual liability and yet still be **covered** because a non-contractual theory may also apply” is contemplated by the Policy itself.

In evaluating Hanover's duty to defend, the district rejected Spec's argument that the Claim potentially includes non-contract claims. The court considered that Spec's was asking the court "to look beyond First Data's demand letters, in violation of the eight corners rule, to find a speculative factual scenario or legal theory in which MasterCard or Visa make a claim directly against Spec's." While acknowledging it had to construe "coverage" liberally and policy exclusions narrowly," the district court stated it was "not required to imagine a legal theory for a potential claim from a third party who has not even sent a demand letter or filed a petition."

*5 The district court was not required to imagine a legal theory for a potential claim. Yet, it was required to frame its analysis in the context of a motion for judgment on the pleadings and the duty to defend. The "central issue" in deciding a motion for judgment on the pleadings is "whether, in the light most favorable to the plaintiff, the complaint states a valid claim for relief." *Great Plains Trust Co. v. Morgan Stanley Dean Witter & Co.*, 313 F.3d 305, 312 (5th Cir. 2002).

The pleadings, viewed in the light most favorable to Spec's, do not unequivocally show Exclusion N excused Hanover's duty to defend under any set of facts or possible theory. The demand letters themselves include references to Spec's "non-complian[ce]" with third-party security standards and not insignificant demands for non-monetary relief, wholly separate from the Merchant Agreement. As explained by Spec's, the non-monetary relief requested in the form of the completion and submission of forms and an Attestation of Compliance from a Qualified Security Assessor "took several months to complete, demanded countless hours of employee time, and required Spec's to hire an outside firm to assist with the effort." The demand letters included Spec's "obligation" for the assessments, and Spec's requirement to "promptly pay" sums to First Data upon request. The allegations, when construed liberally and in the light most favorable to Spec's, implicate theories of negligence and general contract law that imply Spec's liability for the assessments separate and apart from any obligations "based upon, arising out of, or attributable to any actual or alleged liability under" the Merchant Agreement.

Although both Hanover and the district court emphasized the demand letters' references to "Spec's[]" indemnification obligation" found in the Merchant Agreement, this phrase appears in the claim only in connection with First Data's creation of Reserve Accounts. Further, its significance is outweighed by the references to non-contractual theories of liability contained in the letters, which must be construed in favor of Spec's and the duty to defend. Simply put, the district court's assertion that "Spec's fail[ed] to allege any facts that show it would be liable or have any form of privity or obligation to pay damages to First Data for any other reason tha[n] those that arise out of contractual liability" rewrites the allegations, ignoring statements in the demand letters that do not depend upon the Merchant Agreement, such as Spec's negligence in not complying with the Payment Card Industry Data Security requirements and demands for a type of non-monetary relief not contemplated by the Merchant Agreement.

The district court also erred in entering judgment on the pleadings on Count 2 because Hanover did not move for judgment on the pleadings on Spec's breach of contract claim. The Defense Funding Agreement, the subject of Count 2 of the complaint, is independent of the insurance policy claims in Counts 1, 3 and 4. Count 2 alleged Hanover breached the Defense Funding Agreement by refusing to pay Spec's defense expenses – without providing required written notice – all the while asserting that fees incurred in the Tennessee Litigation do not qualify as defense expenses. In its Motion for Judgment on the Pleadings, Hanover did not mention the Defense Funding Agreement; Hanover argued only that the Policy excused it from having to defend Spec's. Consequently, the district court's judgment on the pleadings dismissing all claims and its effective *sua sponte* dismissal of Count 2 was improper. *See, e.g., Davoodi v. Austin Indep. Sch. Dist.*, 755 F.3d 307, 310 (5th Cir. 2014) (noting "district courts should not dismiss claims *sua sponte* without prior notice and opportunity to respond.") (quoting *Carroll v. Fort James Corp.*, 470 F.3d 1171, 1177 (5th Cir. 2006)).

*6 For the foregoing reasons, we **REVERSE** the district court's judgment and **REMAND** for further proceedings.

All Citations

--- Fed.Appx. ----, 2018 WL 3120794

Footnotes

- 1 The Tennessee district court granted Spec's summary judgment motion on July 7, 2017, finding First Data materially breached the Merchant Agreement, as it was not entitled to withhold funds to indemnify itself for the costs associated with the data breaches, and held Spec's is entitled to attorney's fees. See *Spec's Family Partners, Ltd. v. First Data Merch. Servs. Corp.*, No. 2:14-cv-02995-JPM-cgc, 2017 WL 4547168, at *9-10 (W.D. Tenn. July 7, 2017). First Data has filed a notice of appeal.
- 2 Hanover filed a conditional cross-appeal regarding the district court's dismissal as moot of Hanover's request for judicial notice of documents upon which the claim against Spec's was made. Because the district court granted Hanover's motion for judgment on the pleadings, Hanover is not an aggrieved party for purposes of appellate standing, its conditional cross-appeal is improper and therefore will not be considered by this court. See *Subway Equip. Leasing Corp. v. Sims (In re Sims)*, 994 F.2d 210, 214 (5th Cir. 1993); see also *Cooper Indus., Ltd. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 876 F.3d 119, 126 (5th Cir. 2017) (finding a cross-appeal is generally not proper when it is brought to challenge a subsidiary finding or conclusion or when the ultimate judgment is favorable to the party cross-appealing).

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.