PROGRAM MATERIALS
Program #30165
June 11, 2020

Emerging Issues in Cyber Insurance Law

Celesq® AttorneysEd Center
www.celesq.com

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

Emerging Issues in Cyber Insurance Law

- Diane D. Reynolds, Esq.
  - Partner, McElroy, Deutsch, Mulvaney & Carpenter, LLP
- Joyce E. Boyle, Esq.
  - Partner, McElroy, Deutsch, Mulvaney & Carpenter, LLP
- Bradford P. Meisel, Esq.
  - Associate, McElroy, Deutsch, Mulvaney & Carpenter, LLP

Overview

- Cyber Insurance has been available for nearly 20 years.
- However, it remains a relatively new and untested product compared to most other forms of property and casualty coverage and compared to fire, flood, and robbery, cyber-related crime represents uncharted territory for insurers and insureds.
- As a result, the law governing cyber insurance and cybersecurity incidents remains a work in progress and courts have yet to decide significant issues related to cyber insurance coverage.

What Can Cyber Insurance Cover?

- Cyber insurance covers losses and liabilities stemming from cyber attacks.
- In addition to compensating insureds for technological remediation and business interruption resulting from cyberattacks, cyber insurance can cover claims against an entity by affected data subjects and governmental authorities stemming from cyberattacks.

What Kind of Cyberattacks Can Cyber Insurance Cover?

- Cyber Insurance can cover various types of cyberattacks including:
  - Phishing
  - Malware
  - Ransomware
  - Data Breaches
  - Directed Denial of Service (DDoS)

Why Is Cyber Insurance Important?

- Cyberattacks can have serious financial costs stemming from both business interruption and remediation.
- According to a 2016 study by the National Cybersecurity Alliance, approximately 60% of small businesses that suffer a cyberattack close within 6 months.
- According to a 2019 report by IBM and the Ponemon Institute, the average cost of a data breach in the United States was $8.19 M.
- Moreover, newly enacted laws in numerous countries have created significant financial exposure for entities affected by data breaches that failed to comply with stringent data security requirements.

Examples of the Cost of Cyberattacks to Businesses

- The 2017 NotPetya ransomware attack caused an estimated $10 B in damages across the globe.
- International food conglomerate Mondelez and pharmaceutical giant Merck were two prominent victims.
- Mondelez made a $100 M claim under its cyber insurance policy and Merck made a $1.3 B claim under its cyber insurance policy as a result they suffered respectively.

Litigation Regarding Cyber Insurance and the "Act of War" Exception

- Mondelez and Merck's respective cyber insurance carriers denied their claims stemming from the NotPetya ransomware attack under their respective insurance insurance policies' exceptions for "acts of war."
- Both insurance carriers took the position that the NotPetya attack was perpetrated by the Russian government and was therefore an act of war subject to the exception.
- The insurance carriers' denials came after United States and United Kingdom government officials publically blamed Russia for the attack.
- Mondelez and Merck both filed lawsuits challenging their respective insurers' denials.
- Mondelez's case is currently pending in Illinois state court while Merck's case is currently pending in New Jersey state court.

The Applicability of the "Act of War" Exception to Cyber Insurance

- State and federal courts have yet to address the applicability of an insurance policy's "act of war" exception to a cyberattack perpetrated by a foreign government or an agent or ally of a foreign government.
- In other contexts, courts have interpreted insurance policies' "act of war" exceptions to apply to the actions of foreign governments or nongovernmental actors (e.g. terrorist organizations and revolutionary groups) that have usurped power over land and act as de facto governments. See, e.g. Universal Cable Productions, LLC v. Atlantic Specialty Insurance Company, 929 F.3d 1143 (9th Cir. 2019); Pan Am World Airways v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2nd Cir. 1974)

The Future of “Act of War” Exception Litigation With Regard to Cyber Insurance

- In recent years, evidence has linked many cyber attacks to foreign governments such as Russia, Iran, and North Korea and their affiliates.
- Moreover, in some countries such as Russia the lines between government and organized cyber crime syndicates have become blurred.
- In this context, many insurers may be able to develop colorable arguments that a given cyberattack was the work of a foreign government or its affiliates and take the position that it is subject to the ”act of war” exception.
- Therefore, depending how courts ultimately apply this exception in cases involving cyberattacks, some insureds may be well advised to consider purchasing additional insurance coverage for acts of war in order to ensure that they are covered in the event of a cyberattack potentially attributable to a foreign government.

European Union General Data Protection Regulation (GDPR)

- The European Union (EU) General Data Protection Law (GDPR) , which took effect on May 25, 2018 has significantly expanded entities' potential exposure in the event of a data breach.
- GDPR can apply extraterritorially to entities located outside the EU with no physical presence in the EU since it governs "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union."

Key Provisions of GDPR

- In addition to imposing significant information privacy obligations on covered entities, GDPR requires covered entities to implement appropriate technical and organizational measures to protect the security of the personal data they possess and process.
- Violations of GDPR are subject to substantial administrative fines that can total up to 4% of a covered entity's global annual revenue from the last financial year.

The California Consumer Privacy Act (CCPA)

- CCPA took effect on January 1, 2020.
- CCPA applies to any entity that "does business in California" and (A) has annual gross revenues in excess of $25 M; (B) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more customers, households, or devices; or (C) derives 50% or more of its annual revenues from selling customers' personal information.

Key Provisions of CCPA

- In addition to imposing significant information privacy requirements on covered entities, CCPA requires covered entities to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information they possess.
- Violations of the requirement that covered entities implement and maintain reasonable security procedures are subject to a private right of action.

Potential for Additional GDPR and CCPA-Like Laws

- Although there is no federal law analogous to GDPR or CCPA in the United States and most states do not have such laws, legislation that would impose similar requirements and create similar exposure for entities that possess, use, process, or collect personal data have been proposed in Congress and various state legislatures and it is possible that other states and perhaps even Congress may enact such laws in the near future.

Tort Law Exposure for Data Breaches

- Generally, courts have not imposed a common law duty on parties that possess, collect, use, or process personal information to secure that information and protect it from data breaches and other types of cyberattacks. See, e.g. Attias v. CareFirst, Inc., 365 F.Supp.3d 1 (D. D.C. 2019); Cooney v. Chicago Public Schools, 407 Ill.App.3d 358 (Ill. Ct. App. 1st Dist. 2010) .
- However, it is possible that paradigm could shift in the coming months and years.
- For example, the Pennsylvania Supreme Court held in 2018 that employers that collect and store employees' personal data on their computer systems have a common law duty to "exercise reasonable care to protect them against" a data breach or cyberattack affecting such information. Dittman v. UMPC, 196 A.3d 1036, 1047 (Penn. 2018)

Data Breach Notification Laws

- Moreover, all fifty states and the District of Columbia have enacted statutes requiring any entity that owns or licenses their residents' personally identifiable to information inform all affected individuals of a data breach, often within specified time frames ranging from 72 hours under California's statute to 60 days under Texas' statute. See, e.g. Cal. Civ. Code § 1798.82; 815 I.L.C.S. § 530/10; Mass. Gen. Laws § 93H-1; N.J.S.A. 56:8-163; N.C. Gen. Stat. § 75-65; Tex. Bus. & Comm. Code § 521.053.
- While most such laws only require notification if personally identifiable information is acquired, some states, namely New Jersey New York, Connecticut, and Florida, require notification if personally identifiable information is simply accessed.
- Twenty-two such statutes including those in California, Illinois, Massachusetts, New Jersey, North Carolina, and Texas provide a private right of action for violations while the other twenty-nine statutes are enforceable by state Attorneys General or administrative agencies.

What Insurers and Insureds Must Consider in Assessing and Managing Cyber Risk

- Many entities remain largely unprepared or underprepared to defend their organizations in the current cybercrime environment, especially given the apparent escalation in cybercrime during the COVID-19 Pandemic.
- Directors and officers often fail to educate themselves and remain up to date on what must be done to adequately defend their organizations against cybercrime including attacks from sophisticated adversaries including foreign governments and international cybercrime syndicates.

Step #1 for Minimizing Cyber Risk

- Evaluate your organization to determine whether or not every aspect of its operations is in compliance with potentially applicable laws governing their cybersecurity, data protection, and data privacy practices including but not limited to GDPR and CCPA.
- Insureds would be well advised to require that non-compliant insureds bring their policies and practices into compliance with all such laws and non-compliant entities would be well advised to do so on their own volition.

Step #2 for Minimizing Cyber Risk

- Organizations should periodically examine their practices, policies, software, and hardware to determine whether or not any vulnerabilities exist that could cause them to suffer potentially preventable cyberattacks.
- Some such vulnerabilities may be technical in nature such as those involving software or hardware.
- Others may involve the unnecessary utilization of high-risk technologies such as inadequately secured cloud computing services or Internet of Things (IoT) connected devices or inadequate employee technology use or monitoring policies and procedures.

Step #3 for Minimizing Cyber Risks

- Insureds should hire a qualified third party to conduct a cyber risk analysis on at least an annual basis and document its findings.
- Insurers should consider requiring their insureds to do so and review the findings.

Step #4 for Minimizing Cyber Risks

- Insureds and insurers alike should consider creating an interdisciplinary team of outside professionals to conduct cybersecurity risk assessments and remediate vulnerabilities and cybersecurity incidents.
- Such an interdisciplinary team will ideally consist of technical subject matter experts as well as outside counsel with experience in both insurance and cybersecurity/information privacy law.
- In addition to fostering sharing of expertise and providing economies of scale, such an approach can cloak the risk assessment process in attorney-client or work-product privilege and shield information regarding the process from discovery in the event of litigation or administrative proceedings.

How Insurers Can Respond to their Insureds' Cybersecurity Risk

- If an insured is found to have failed to address detected vulnerabilities or comply with applicable information security or privacy laws, insurers may have a tangible basis on which to increase premiums, refuse to renew a policy, or deny initial coverage.
- Insurers can also incentivize compliance with data security assessment recommendations through premium reductions.
- Therefore, insureds seeking to obtain affordable cyber insurance coverage would be well advised to follow the recommended steps for minimizing cyber risks.

Questions

 KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

West's North Carolina General Statutes Annotated
Chapter 75. Monopolies, Trusts and Consumer Protection (Refs & Annos)
Article 2a. Identity Theft Protection Act

N.C.G.S.A. § 75-65

§ 75-65. Protection from security breaches

Effective: October 1, 2009
Currentness

(a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

(c) The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

(d) The notice shall be clear and conspicuous. The notice shall include all of the following:

(1) A description of the incident in general terms.

(2) A description of the type of personal information that was subject to the unauthorized access and acquisition.

(3) A description of the general acts of the business to protect the personal information from further unauthorized access.

(4) A telephone number for the business that the person may call for further information and assistance, if one exists.

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(6) The toll-free numbers and addresses for the major consumer reporting agencies.

(7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.

(3) Telephonic notice provided that contact is made directly with the affected persons.

(4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

a. E-mail notice when the business has an electronic mail address for the subject persons.

b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.

c. Notification to major statewide media.

(e1) In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

(g) Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable.

(h) A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in compliance with the Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration; and any revisions, additions, or substitutions relating to any of the said interagency guidance, shall be deemed to be in compliance with this section.

(i) A violation of this section is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

(j) Causes of action arising under this Article may not be assigned.

Credits

Added by S.L. 2005-414, § 1, eff. Dec. 1, 2005. Amended by S.L. 2009-355, § 2, eff. Oct. 1, 2009; S.L. 2009-573, § 10, eff. Oct. 1, 2009.

Notes of Decisions (1)

N.C.G.S.A. § 75-65, NC ST § 75-65

The statutes and Constitution are current through the end of the 2019 Regular Session of the General Assembly, subject to changes made pursuant to direction of the Revisor of Statutes.

End of Document

KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

New Jersey Statutes Annotated
Title 56. Trade Names, Trade-Marks and Unfair Trade Practices
Chapter 8. Frauds, Etc., in Sales or Advertisements of Merchandise (Refs & Annos)

N.J.S.A. 56:8-163

56:8-163. Disclosure of breach of security of computerized records; report to Division of State Police; exception; forms of notification

Effective: September 1, 2019
Currentness

a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

b. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

c. (1) Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

d. For purposes of this section, notice may be provided by one of the following methods:

(1) Written notice;

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 101 of the federal "Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001); or

(3) Substitute notice, if the business or public entity demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the business or public entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

(a) E-mail notice when the business or public entity has an e-mail address;

(b) Conspicuous posting of the notice on the Internet web site page of the business or public entity, if the business or public entity maintains one; and

(c) Notification to major Statewide media.

e. Notwithstanding subsection d. of this section, a business or public entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and is otherwise consistent with the requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the business or public entity notifies subject customers in accordance with its policies in the event of a breach of security of the system.

f. In addition to any other disclosure or notification required under this section, in the event that a business or public entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the business or public entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s.1681a), of the timing, distribution and content of the notices.

g. (1) Notwithstanding subsection d. of this section, in the case of a breach of security involving a user name or password, in combination with any password or security question and answer that would permit access to an online account, and no other personal information as defined in section 10 of P.L.2005, c. 226 (C.56:8-161), the business or public entity may provide the notification in electronic or other form that directs the customer whose personal information has been breached to promptly change any password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the business or public entity and all other online accounts for which the customer uses the same user name or email address and password or security question or answer.

(2) Any business or public entity that furnishes an email account shall not provide notification to the email account that is subject to a security breach. The business or public entity shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the customer online when the customer is connected to the online account from an Internet Protocol address or online location from which the business or public entity knows the customer customarily accesses the account.

Credits

L.2005, c. 226, § 12, eff. Jan. 1, 2006. Amended by L.2019, c. 95, § 2, eff. Sept. 1, 2019.

N. J. S. A. 56:8-163, NJ ST 56:8-163
Current with laws through L.2020, c. 17. All 2020 amendments, relating to emergency COVID-19 legislation, were implemented using the Advanced Law copy of the bill and therefore are subject to change upon issuance of the Pamphlet Law by the Office of Legislative Services.

End of Document

 KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

West's Smith-Hurd Illinois Compiled Statutes Annotated
Chapter 815. Business Transactions
Deceptive Practices
Act 530. Personal Information Protection Act

815 ILCS 530/10

530/10. Notice of breach; notice to Attorney General

Effective: January 1, 2020
Currentness

§ 10. Notice of breach; notice to Attorney General.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":

(A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate

with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(e)(1) This subsection does not apply to data collectors that are covered entities or business associates and are in compliance with Section 50.

(2) Any data collector required to issue notice pursuant to this Section to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including:

(A) A description of the nature of the breach of security or unauthorized acquisition or use.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the data collector has taken or plans to take relating to the incident.

Such notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers pursuant to this Section. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible.

Upon receiving notification from a data collector of a breach of personal information, the Attorney General may publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.

Credits

P.A. 94-36, § 10, eff. Jan. 1, 2006. Amended by P.A. 94-947, § 5, eff. June 27, 2006; P.A. 97-483, § 5, eff. Jan. 1, 2012; P.A. 99-503, § 5, eff. Jan. 1, 2017; P.A. 100-201, § 800, eff. Aug. 18, 2017; P.A. 101-343, § 5, eff. Jan. 1, 2020.

Notes of Decisions (5)

815 I.L.C.S. 530/10, IL ST CH 815 § 530/10
Current through P.A. 101-629. Some statute sections may be more current, see credits for details.

End of Document

KeyCite Yellow Flag - Negative Treatment
Proposed Legislation

West's Annotated California Codes
Civil Code (Refs & Annos)
Division 3. Obligations (Refs & Annos)
Part 4. Obligations Arising from Particular Transactions (Refs & Annos)
Title 1.81. Customer Records (Refs & Annos)

West's Ann.Cal.Civ.Code § 1798.82

§ 1798.82. Person or business who owns or licenses computerized data including personal information; breach of security of the system; disclosure requirements

Effective: January 1, 2020
Currentness

(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO] Date: [insert date]

NOTICE OF DATA BREACH

What Happened?

What Information Was Involved?

What We Are Doing.

What You Can Do.

Other Important Information.

[insert other important information]

Call [telephone number] or go to [internet website]

For More
Information.

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that people whose information has been breached may take to protect themselves.

(C) In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). [1] However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, “personal information” means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

(i)(1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(k) For purposes of this section, “encryption key” and “security credential” mean the confidential key or process designed to render data usable, readable, and decipherable.

(*l*) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Credits

(Added by Stats.2002, c. 1054 (A.B.700), § 4, operative July 1, 2003. Amended by Stats.2007, c. 699 (A.B.1298), § 6; Stats.2011, c. 197 (S.B.24), § 2; Stats.2013, c. 396 (S.B.46), § 2; Stats.2014, c. 855 (A.B.1710), § 2, eff. Jan. 1, 2015; Stats.2015, c. 522 (A.B.964), § 2, eff. Jan. 1, 2016; Stats.2015, c. 532 (S.B.34), § 2, eff. Jan. 1, 2016; Stats.2015, c. 543 (S.B.570), § 2.3, eff. Jan. 1, 2016; Stats.2016, c. 86 (S.B.1171), § 21, eff. Jan. 1, 2017; Stats.2016, c. 337 (A.B.2828), § 2, eff. Jan. 1, 2017; Stats.2019, c. 750 (A.B.1130), § 3, eff. Jan. 1, 2020.)

Notes of Decisions (7)

Footnotes

1 For public law sections classified to the U.S.C.A., see USCA-Tables.

West's Ann. Cal. Civ. Code § 1798.82, CA CIVIL § 1798.82

Current with urgency legislation through Ch. 3 of 2020 Reg.Sess

End of Document

KeyCite Yellow Flag - Negative Treatment
Declined to Follow by In re Intel Corp. CPU Marketing, Sales Practices and Products Liability Litigation, D.Or., March 27, 2020

365 F.Supp.3d 1
United States District Court, District of Columbia.

Chantal ATTIAS, et al., Plaintiffs,
v.
CAREFIRST, INC., et al., Defendants.

Case No. 15-cv-00882 (CRC)
|
Signed 01/30/2019

Synopsis

Background: Insureds brought putative class action against health insurer, asserting claims for breach of contract, negligence, and violation of various state consumer-protection statutes, after their personal information was stolen during data breach. The District Court, 199 F.Supp.3d 193, granted insurer's motion to dismiss. Insureds appealed. The Court of Appeals, 865 F.3d 620, reversed. On remand, insurer moved to dismiss for failure to state claim.

Holdings: The District Court, Christopher R. Cooper, J., held that:

[1] district court had diversity jurisdiction;

[2] only insureds who had suffered actual fraud stated claim for actual damages;

[3] insureds failed to allege duty on part of insurer;

[4] insureds failed to state claim for unjust enrichment;

[5] intentional breach of contract was not punishable as an unlawful trade practice under the District of Columbia Consumer Protection Procedures Act (DCCPPA); and

[6] insurer's data-security services were not exempt from provisions of Maryland Consumer Protection Act (MCPA) as "professional services."

Motion to dismiss granted in part and denied in part.

West Headnotes (35)

[1] **Federal Courts** Citizens of District of Columbia or territories

Federal Courts Class and derivative actions

Federal Courts Insurers

Under Class Action Fairness Act (CAFA), district court had diversity jurisdiction over state-law claims against operator of group of health insurance companies arising from alleged data breach; plaintiffs estimated that there were more than one million class and sub-class members, parties were residents of District of Columbia and two states and had sued operator and its affiliates doing business in those three places, and amount in controversy almost certainly exceeded $5 million. 28 U.S.C.A. § 1332(d)(2), (5)(B).

[2] **Federal Courts** Substance or procedure; determinativeness

A federal court sitting in diversity must apply the substantive law of the jurisdiction in which it sits.

[3] **Damages** Allegations as to damage in general

Plaintiffs may satisfy the Article III injury-in-fact requirement of standing and yet fail to adequately plead damages for a particular cause of action. U.S. Const. Art. 3.

[4] **Contracts** Grounds of action

Under District of Columbia law, actual loss or damage is an essential element for a breach of contract cause of action.

[5] **Contracts** Grounds of action

Under District of Columbia law, the mere danger of future harm, unaccompanied by present injury, will not support a breach of contract action.

[6] **Negligence** Nature of injury

Under District of Columbia law, to maintain an action for negligence or negligence per se, a plaintiff must allege more than speculative harm from defendant's allegedly negligent conduct.

[7] **Fraud** Injury and causation

Under District of Columbia law, provable damages is an essential element of common law fraud.

[8] **Fraud** Elements of Constructive Fraud

Under District of Columbia law, constructive fraud differs from actual fraud only in that the misrepresentation of material fact is not made with the intent to mislead, but is made innocently or negligently.

[9] **Fraud** Injury and causation

Under District of Columbia law, constructive fraud requires actual damages.

[10] **Fraud** Fiduciary or confidential relations

Under District of Columbia law, a claim for a breach of the duty of confidentiality is equivalent to a claim for a breach of a fiduciary duty.

1 Cases that cite this headnote

[11] **Fraud** Injury and causation

Under District of Columbia law, a breach of a fiduciary duty requires a showing of injury or damages.

1 Cases that cite this headnote

[12] **Antitrust and Trade Regulation** Pleading

Under the Maryland Consumer Protection Act, a plaintiff must plead actual injury or harm. Md. Code Ann., Com. Law § 13-408(a).

[13] **Antitrust and Trade Regulation** Reliance; causation; injury, loss, or damage

For a plaintiff to articulate a cognizable injury under the Maryland Consumer Protection Act, the injury must be objectively identifiable, meaning the consumer must have suffered an identifiable loss, measured by the amount the consumer spent or loss as a result of his or her reliance on the sellers' misrepresentation. Md. Code Ann., Com. Law § 13-408(a).

[14] **Antitrust and Trade Regulation** Reliance; causation; injury, loss, or damage

The Virginia Consumer Protection Act requires a plaintiff to plead actual loss in order to bring a suit for damages under the Act. Va. Code Ann. § 59.1-204(A).

[15] **Antitrust and Trade Regulation** Health care and medical insurance

Insurance Privacy of Information

Insurance Negligence in general

Insurance Fraud or misrepresentation; concealment

Under District of Columbia law, mere threat of misuse of insureds' personal information as a result of data breach suffered by health insurer was insufficient to state claim for actual damages against insurer on claims of breach of contract, negligence, negligence per se, fraud, constructive fraud, breach of duty of confidentiality, violation of Maryland Consumer Protection Act, violation of Virginia Consumer Protection Act, and violation of District of Columbia Data Breach Notification Act. D.C. Code § 28-3853(a); Md. Code Ann., Com. Law § 13-408(a); Va. Code Ann. § 59.1-204(A).

[16] **Antitrust and Trade Regulation** Health care and medical insurance

Insurance Privacy of Information

Insurance Negligence in general

Insurance Fraud or misrepresentation; concealment

Under District of Columbia law, claim that insureds had experienced tax-refund fraud as a result of data breach suffered by health insurer was sufficient to state claim for actual damages against insurer on claims of breach of contract, negligence, negligence per se, fraud, constructive fraud, breach of duty of confidentiality, violation of Maryland Consumer Protection Act, violation of Virginia Consumer Protection Act, and violation of District of Columbia Data Breach Notification Act. D.C. Code § 28-3853(a); Md. Code Ann., Com. Law § 13-408(a); Va. Code Ann. § 59.1-204(A).

[17] **Antitrust and Trade Regulation** Health care and medical insurance

Insurance Privacy of Information

Insurance Negligence in general

Insurance Fraud or misrepresentation; concealment

Under District of Columbia law as predicted by the district court, claim that insureds were harmed by loss of benefit of the bargain as a result of data breach suffered by health insurer was insufficient to state claim for actual damages against insurer on claims of breach of contract, negligence, negligence per se, fraud, constructive fraud, breach of duty of confidentiality, violation of Maryland Consumer Protection Act, violation of Virginia Consumer Protection Act, and violation of District of Columbia Data Breach Notification Act, where insureds did not allege actual misuse of their exposed personal information. D.C. Code § 28-3853(a); Md. Code Ann., Com. Law § 13-408(a); Va. Code Ann. § 59.1-204(A).

1 Cases that cite this headnote

[18] **Antitrust and Trade Regulation** Health care and medical insurance

Insurance Privacy of Information

Insurance Negligence in general

Insurance Fraud or misrepresentation; concealment

Under District of Columbia law, time and money that insureds spent protecting against future identity theft following data breach suffered by health insurer did not constitute actual damage in their own right on claims of breach of contract, negligence, negligence per se, fraud, constructive fraud, breach of duty of confidentiality, violation of Maryland Consumer Protection Act, violation of Virginia Consumer Protection Act, and violation of District of Columbia Data Breach Notification Act. D.C. Code § 28-3853(a); Md. Code Ann., Com. Law § 13-408(a); Va. Code Ann. § 59.1-204(A).

[19] **Antitrust and Trade Regulation** Health care and medical insurance

Damages Insurance Practices

Insurance Privacy of Information

Insurance Negligence in general

Insurance Fraud or misrepresentation; concealment

Under District of Columbia law, claim that insureds had experienced emotional distress as a result of data breach suffered by insurer was sufficient to state claim for actual damages against health insurer on claims of negligence, negligence per se, fraud, constructive fraud, and violation of Maryland Consumer Protection Act; insureds sought only ancillary damages for related mental distress, and there was no showing of economic harm. Md. Code Ann., Com. Law § 13-408(a).

[20] **Damages** Negligent Infliction of Emotional Distress

Damages Physical illness, impact, or injury; zone of danger

Under District of Columbia law, to state a claim of negligence where emotional distress is the only injury suffered, the plaintiff must satisfy either the "zone of physical danger" rule or the "special relationship and undertaking" rule.

[21] **Insurance** Privacy of Information

Insurance Negligence in general

Insurance Fraud or misrepresentation; concealment

Insureds failed to allege duty on part of health insurer to safeguard insureds' data separate from insurer's contractual duties, and thus insureds could not maintain claims against insurer under District of Columbia law for negligence, negligence per se, fraud, constructive fraud, and breach of duty of confidentiality arising from data breach suffered by insurer; complaint alleged no facts separable from terms of contract upon which tort could independently rest and identified no duty independent of that arising out of contract itself.

1 Cases that cite this headnote

[22] **Torts** Contractual duty

Under District of Columbia law, the failure to perform a contractual obligation typically does not give rise to a cause of action in tort.

[23] **Torts** Duty, breach, or wrong independent of contract

Under District of Columbia law, for a plaintiff to recover in tort for conduct that also constitutes a breach of contract, the tort must exist in its own right independent of the contract, and any duty upon which the tort is based must flow from considerations other than the contractual relationship.

2 Cases that cite this headnote

[24] **Negligence** Necessity and Existence of Duty

Under District of Columbia law, whether a duty exists is the result of a variety of considerations, including the foreseeability of harm and the nature of the relationship between the parties.

[25] **Negligence** Protection against acts of third persons

Negligence Protection against acts of third persons

Under District of Columbia law, if the relationship between the parties strongly suggests a duty of protection, then specific evidence of foreseeability is less important, whereas if the relationship is not of a type that entails a duty of protection, then the evidentiary hurdle is higher.

[26] **Insurance** Fiduciary relationships in general

District of Columbia law does not consider the relationship between insurer and insured a fiduciary relationship as a matter of law.

2 Cases that cite this headnote

[27] **Insurance** Relations Between Parties; Implied Terms

Under District of Columbia law, the relationship between parties to an insurance contract is generally considered contractual in nature.

2 Cases that cite this headnote

[28] **Fraud** Fiduciary or confidential relations

Under District of Columbia law, determining whether a fiduciary relationship exists requires a searching inquiry into the nature of the relationship, the promises made, the types of services or advice given and the legitimate expectations of the parties.

[29] **Fraud** Fiduciary or confidential relations

Under District of Columbia law, a fiduciary relationship could exist where circumstances show that the parties extended their relationship beyond the limits of the contractual obligations to a relationship founded upon trust and confidence.

1 Cases that cite this headnote

[30] **Fraud** Effect of existence of remedy by action on contract

District of Columbia law requires that the factual basis for a fraud claim be separate from any breach of contract claim that may be asserted.

[31] **Implied and Constructive Contracts** Effect of Express Contract

Under District of Columbia law, insureds failed to state claim against health insurer for unjust enrichment arising from breach suffered by insurer, where insureds did not allege that insurance contract was invalid and unenforceable.

[32] **Implied and Constructive Contracts** Effect of Express Contract

Under District of Columbia law, the existence of a valid contract precludes a claim for unjust enrichment.

[33] **Federal Civil Procedure** Alternate, Hypothetical and Inconsistent Claims

Pleading unjust enrichment as an alternative to a claim for breach of contract requires an allegation that the contract is invalid and unenforceable.

[34] **Antitrust and Trade Regulation** Contractual relationships and breach of contract in general

An intentional breach of contract is not punishable as an unlawful trade practice under the District of Columbia Consumer Protection Procedures Act (DCCPPA) simply because the breach was intended when the contract was formed. D.C. Code § 28-3901 et seq.

1 Cases that cite this headnote

[35] **Antitrust and Trade Regulation** Other particular professions

Health insurer's data-security services were not exempt from provisions of Maryland Consumer Protection Act (MCPA) as "professional services"; gathering and storing consumers' private information was ancillary to provision of health insurance coverage. Md. Code Ann., Com. Law § 13-104(1).

Attorneys and Law Firms

***4** Christopher T. Nace, Matthew Andrew Nace, Paulson & Nace, PLLC, Jonathan B. Nace, Nidel & Nace, PLLC, Washington, DC, Matthew W. Stonestreet, Pro Hac Vice, Troy Nino Alexander Giatras, Giatras Law Firm, PLLC, Charleston, WV, for Plaintiffs.

Matthew O. Gatewood, Eversheds Sutherland (US) LLP, Washington, DC, Robert D. Owen, Sutherland Asbil & Brennan, LLP, New York, NY, Kristine M. Maher, Graydon, Head & Ritchey, LLP, Cincinnati, OH, for Defendants.

MEMORANDUM OPINION

CHRISTOPHER R. COOPER, United States District Judge

In May 2015, the District of Columbia-area health insurer CareFirst announced that it had suffered a data breach that compromised the personal information of millions of its policyholders. Plaintiffs in this putative class action are among those whose data was accessed. They seek compensation for the breach through both tort- and contract-based claims under District of Columbia law, as well as statutory claims under several D.C., Maryland, and Virginia consumer-protection laws.

Common to all of plaintiffs' claims is the assertion that they have been injured by CareFirst's failure to protect their personal information from exposure. The alleged injuries do not, for the most part, involve actual misuse of their personal information. Plaintiffs instead claim that the data breach resulted in an increased *risk* of identity theft and the need for prophylactic expenditures—on credit monitoring services and the like—to reduce that risk. They also contend that CareFirst's failure to protect their personal information resulted in a contractual injury because they did not receive the full value of the policies they purchased. And they say they have suffered emotional distress in dealing with the breach.

The Court previously dismissed plaintiffs' claims for lack of Article III standing, finding that they had failed to allege a non-speculative injury-in-fact. The D.C. Circuit reversed and remanded. CareFirst now moves to dismiss the operative second amended complaint under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim.

The Court will grant the motion in large part. After briefly recounting the factual and procedural background, the Court will begin by confirming that it has diversity jurisdiction over the case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). It will then explain its conclusion that, while plaintiffs' alleged injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the "actual damages" element of nine of their state-law causes of action. The Court will then move to the interplay between plaintiffs' tort and contract claims, finding that the parties' non-fiduciary contractual relationship independently forecloses tort liability based on the allegations in the complaint. Finally, the Court will address issues specific to plaintiffs' ***6** unjust enrichment claim and their claims under the District of Columbia Consumer Protection Procedures Act and the Maryland Consumer Protection Act.

At the end of the day, the Court will dismiss all of plaintiffs' claims except for a breach of contract claim and a Maryland Consumer Protection Act claim brought by the only two plaintiffs (Kurt and Connie Tringler of Maryland) who have plausibly alleged actual misuse of personal information resulting from the data breach. In reaching this outcome, the Court acknowledges the difficulty of applying traditional tort and contract principles in the contemporary context of data security. It also recognizes that courts across the country have divided on a number of important legal issues that frequently arise in data breach litigation. The Court has attempted to illuminate some of these divisions in this opinion.

I. Background

Seven plaintiffs bring this putative class action against CareFirst and certain of its affiliates doing business in the District of Columbia, Maryland, and Virginia. Second Am. Class Action Compl. ("SAC"), ECF No. 9.[1] CareFirst operates a group of health insurance companies providing coverage to more than one million individuals in the District of Columbia, Maryland, and Virginia. Id. ¶¶ 5–8, 23. Plaintiffs are residents of the District of Columbia, Maryland, and Virginia, and customers and insureds of CareFirst. Id. ¶¶ 1–4, 25. When customers purchase health insurance through CareFirst, they provide the company certain personal information, including their names, credit card numbers, addresses, and social security numbers. Id. ¶¶ 26–27. CareFirst promises, explicitly or implicitly, to keep this information protected. Id. ¶¶ 28–29. CareFirst allegedly failed to properly encrypt some of the data entrusted to its care, id. ¶ 31, and in June 2014, CareFirst suffered a cyberattack, id. ¶ 33. It learned of the attack in April 2015 and notified its customers, including plaintiffs, the following month. Id. ¶¶ 35–36.

Plaintiffs initiated this action shortly after learning of the data breach and filed the operative second amended complaint in July 2015. They bring eleven claims: breach of contract (Count I), negligence (Count II), violation of the District of Columbia Consumer Protection Procedures Act (Count III), violation of the District of Columbia Data Breach

Notification Statute (Count IV), violation of the Maryland Consumer Protection Act (Count V), violation of the Virginia Consumer Protection Act (Count VI), fraud (Count VII), negligence *per se* (Count VIII), unjust enrichment (Count IX), breach of the duty of confidentiality (Count X), and constructive fraud (Count XI). They allege that they "have suffered economic and non-economic loss in the form of mental and emotional pain and suffering and aguish [sic] as a result of Defendants' failures" to secure plaintiffs' confidential information. SAC ¶ 38. The Tringlers specifically allege that they have experienced "tax-refund fraud" as a result of the data breach. Id. ¶ 57. And all plaintiffs allege that they "face years of constant surveillance of their financial and personal records, monitoring, and loss of rights." Id. ¶ 56.

CareFirst moved to dismiss the complaint for lack of subject matter jurisdiction under Rule 12(b)(1) and failure to state a claim under Rule 12(b)(6). The Court granted the 12(b)(1) motion on the ground that plaintiffs had not identified an "actual or imminent" injury as is necessary ***7** to satisfy the injury-in-fact requirement of constitutional standing. In so doing, the Court observed that most of the plaintiffs had not alleged that their personal information had actually been misused in any way. Nor had they explained how the information taken (which CareFirst averred did not include financial information or social security numbers) could readily be used to assume their identities. Based on these factors, the Court adopted the principle that most other courts have followed in similar cases, including a Maryland federal class action brought by another set of CareFirst customers stemming from the same breach: "Absent facts demonstrating a substantial risk that stolen data has been or will be misused in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from wh[ich] the information was taken." Attias v. CareFirst, Inc., 199 F.Supp.3d 193, 197 (D.D.C. 2016). The Court further held that plaintiffs' other asserted injuries were also insufficient to meet the injury-in-fact requirement of standing. Those harms included (1) expenditures on credit-monitoring services to prevent future identity theft; (2) some indeterminate overpayment for their insurance coverage; (3) loss of the intrinsic value of the stolen personal information; and (4) violation of their statutory rights under various consumer protection laws. Id. at 202–03.

The D.C. Circuit reversed and remanded, finding that plaintiffs had plausibly alleged a substantial risk of identity theft flowing from the data breach, which was enough to meet "the light burden of proof the plaintiffs bear at the pleading stage" of the case. Attias v. CareFirst, Inc., 865 F.3d 620, 627–28 (D.C. Cir. 2017). The Circuit declined to reach CareFirst's alternative argument that plaintiffs had failed to state a claim under Rule 12(b)(6). Id. at 629–30. It did so because this Court had reserved judgment on a second threshold jurisdictional question—whether diversity jurisdiction exists under the Class Action Fairness Act, 28 U.S.C. § 1332(d)—which the Circuit could not answer on the record before it. Attias, 865 F.3d at 629–30.

Venturing once more into the breach, CareFirst has now renewed its 12(b)(6) motion before this Court. Mem. in Supp. of Defs.' Mot. to Dismiss ("MTD"), ECF No. 44-1. Plaintiffs oppose the motion. Pls.' Opp'n to MTD ("Opp'n"), ECF No. 45. The Court held a hearing on November 5, 2018, and the motion is now ripe for resolution.

II. Standard of Review

In analyzing a motion to dismiss under Rule 12(b)(6), the Court must determine whether the complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " Ashcroft v. Iqbal, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). This requires "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. To make this determination, the Court "must take all of the factual allegations in the complaint as true." Id. It also must "construe[] the complaint liberally in the plaintiff's favor with the benefit of all reasonable inferences derived from the facts alleged." Stewart v. Nat'l Educ. Ass'n, 471 F.3d 169, 173 (D.C. Cir. 2006). Finally, the Court may only "consider the facts alleged in the complaint, documents attached thereto or incorporated therein, and matters of which it may take judicial notice." Id.

III. Jurisdiction

[1] The Court turns first to the jurisdictional question that it previously left unresolved: whether it has diversity jurisdiction over plaintiffs' eleven state-law ***8** claims under the Class Action Fairness Act ("CAFA"). It does. "CAFA gives federal courts jurisdiction over certain class actions, ... if the class has more than 100 members, the parties are minimally diverse, and the amount in controversy exceeds $ 5 million." Dart Cherokee Basin Operating Co., LLC v. Owens, 574 U.S. 81, 135 S.Ct. 547, 552, 190 L.Ed.2d 495 (2014) (citing 28 U.S.C. §§ 1332(d)(2), (5)(B)). Beginning

with the first requirement, plaintiffs estimate that there are more than one million class and sub-class members, SAC ¶ 63, and CareFirst does not contest that number for purposes of this motion, Hr'g Tr. at 3:2–3:14. Second, the parties are minimally diverse because "any member of a class of plaintiffs is a citizen of a State different from any defendant," 28 U.S.C. § 1332(d)(2)(A): The plaintiffs are residents of the District of Columbia, Maryland, and Virginia and have sued CareFirst and its affiliates doing business in those three places. And third, the amount in controversy almost certainly exceeds the $ 5 million threshold. Under CAFA, the Court aggregates the individual claims of class members. Here, even if individual class members' claims are worth just $ 5 each, they would satisfy the amount-in-controversy requirement. But it's likely that the value of their claims is much more. For example, plaintiffs have brought claims under the District of Columbia Consumer Protection Procedures Act, D.C. Code Ann. § 28-3901 *et seq.*, which provides statutory damages of $ 1,500 per violation, and the Virginia Consumer Protection Act ("VCPA"), Va. Code Ann. § 59.1-196 *et seq.*, which entitles successful plaintiffs to $ 500 to $ 1,000 per violation. SAC ¶¶ 90(d), 115. Although plaintiffs do not provide a breakdown of the numbers in each subclass, it's hard to imagine a distribution that would not satisfy the amount-in-controversy requirement based solely on these statutory claims. In any event, neither party questions that the amount in controversy exceeds $ 5 million. See SAC ¶ 10; Hr'g Tr. at 3:2–3:4; Dart Cherokee, 135 S.Ct. at 553 (explaining that amount-in-controversy allegation should be accepted where not questioned by either party).

Accordingly, because the prospective class has more than 100 members, the parties are minimally diverse, and the amount in controversy exceeds $ 5 million, this Court has diversity jurisdiction under CAFA. See Dart Cherokee, 135 S.Ct. at 552.

IV. Analysis

[2] "A federal court sitting in diversity must apply the substantive law of the jurisdiction in which it sits." Metz v. BAE Sys. Tech. Sol. & Servs. Inc., 774 F.3d 18, 21–22 (D.C. Cir. 2014). Here, that jurisdiction is the District of Columbia. [2] This means that the Court is bound by decisions of the District of Columbia Court of Appeals—the highest court in D.C.—interpreting D.C. law. Id. This requirement is all the more salient in a data-breach case like this because federal courts across the country have applied the relevant state law to claims arising out of data breaches to very different effect. In the absence of a decision by the District of Columbia Court of Appeals, the Court's role in interpreting and applying D.C. law is to achieve the same outcome it believes would result if the District's highest court considered this case. Id.

As will follow, the Court first concludes that all plaintiffs but the Tringlers have failed to allege, as they must, actual damages ***9** for nine of their eleven claims. The Court then finds that plaintiffs' contractual relationship with CareFirst precludes the rest of their claims: their tort claims because they fail to allege an independent duty to safeguard private information; their unjust enrichment claim because they fail to allege that their contract is invalid or unenforceable; and their D.C. Consumer Protection Procedures Act claim because they fail to allege any unlawful trade practice beyond the breach of contract itself. In the end, only the Tringlers remain and they are left only with their breach of contract claim in Count I and their Maryland Consumer Protection Act claim in Count V.

A. Whether plaintiffs have adequately alleged damages for nine of their eleven claims

CareFirst moves to dismiss the following nine of plaintiffs' claims for failure to allege actual damages: (1) breach of contract; (2) negligence and (3) negligence *per se*; (4) fraud and (5) constructive fraud; (6) breach of the duty of confidentiality; violations of the (7) Maryland and (8) Virginia Consumer Protection Acts; and violation of the (9) District of Columbia Breach Notification Statute. MTD at 6–10. Plaintiffs counter that CareFirst simply camouflages the "the exact same argument" regarding speculative harm previously rejected by the D.C. Circuit in deciding that they have adequately pled an injury-in-fact for purposes of standing. Opp'n at 1, 5.

[3] The D.C. Circuit's standing ruling does not control whether plaintiffs have alleged actual harm for purposes of their state-law claims. See id. at 6. Plaintiffs may satisfy the Article III injury-in-fact requirement and yet fail to adequately plead damages for a particular cause of action. For example, in Krottner v. Starbucks Corp., 406 F. App'x 129 (9th Cir. 2010), the Ninth Circuit explained that its holding in a concurrently published opinion that the plaintiffs "pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of their state-law claims" arising out of the theft of a company laptop containing the confidential personal information of thousands of Starbucks employees. Id. at

131.[3] The court concluded that, despite having Article III standing based on the risk of future identity theft, the employees failed to state a negligence claim because, under the relevant state law, "[t]he mere danger of future harm, unaccompanied by present damage, will not support a negligence action." Id. (citation omitted). So too here. Although plaintiffs have successfully pled an injury-in-fact sufficient to support federal constitutional standing, they must still plead a proper cause of action under the relevant D.C. or state law.

With that issue aside, the Court now turns to the merits of CareFirst's argument that nine causes of action should be dismissed for failure to plead damages under the applicable state laws.

1. Plaintiffs must allege actual damages for nine of their causes of action

All but two of plaintiffs' claims require allegations of actual damages.

a. Breach of contract

[4] **[5]** Under District of Columbia law, actual loss or damage is an essential element for a breach of contract cause of action. See Cahn v. Antioch Univ., 482 A.2d 120, 130 (D.C. 1984) ("It is clear in ***10** contract law that a plaintiff is not required to prove the amount of his damages precisely; however, the fact of damage and a reasonable estimate must be established." (quoting W.G. Cornell Co. of Wash., D.C. v. Ceramic Coating Co., Inc., 626 F.2d 990, 993 (D.C. Cir. 1980))); Sloan v. Urban Title Servs., Inc., 689 F.Supp.2d 123, 133 & 133 n.7 (D.D.C. 2010) ("Both District and Virginia law require proof of injury (*i.e.*, damages) as an element of claims for breach of contract[.]" (citing Osbourne v. Capital City Mortg. Corp., 727 A.2d 322, 324–25 (D.C. 1999))). The mere danger of future harm, unaccompanied by present injury, will not support a breach of contract action. See Sloan, 689 F.Supp.2d at 134–35.

b. Negligence and negligence *per se*

[6] Under D.C. law, "[t]o maintain an action for negligence, a plaintiff must allege more than speculative harm from defendant's allegedly negligent conduct." Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 708 (D.C. 2009); see also Hillbroom v. PricewaterhouseCoopers LLP, 17 A.3d 566, 573 (D.C. 2011) ("[T]he mere breach of a professional duty, causing only nominal damages, speculative harm, or the threat of future harm—not yet realized—does not suffice to create a cause of action for negligence." (quoting Knight v. Furlow, 553 A.2d 1232, 1235 (D.C. 1989))). The same is true for a negligence *per se* action. See Tolson v. The Hartford Fin. Servs. Grp., Inc., 278 F.Supp.3d 27, 36 (D.D.C. 2017) (explaining that plaintiff "would still have to prove that she was *injured* " for her negligence *per se* claim).

c. Fraud and constructive fraud

[7] **[8]** **[9]** Next, "provable damages" is also an "essential element[ ] of common law fraud" in the District. Kitt v. Capital Concerts, Inc., 742 A.2d 856, 860–61 (D.C. 1999) (citing Dresser v. Sunderland Apartments Tenants Ass'n, Inc., 465 A.2d 835, 839 (D.C. 1983)); see also Wetzel v. Capital City Real Estate, LLC, 73 A.3d 1000, 1002–03 (D.C. 2013). "Constructive fraud differs from actual fraud only in that the misrepresentation of material fact is not made with the intent to mislead, but is made innocently or negligently." De May v. Moore & Bruce, L.L.P., 584 F.Supp.2d 170, 185 (D.D.C. 2008) (quoting Nguyen v. Voorthuis Opticians, Inc., 478 F.Supp.2d 56, 64 (D.D.C. 2007)). As such, constructive fraud also requires actual damages.

d. Breach of the duty of confidentiality

[10] **[11]** A claim for a breach of the duty of confidentiality is equivalent to a claim for a breach of a fiduciary duty. See Democracy Partners v. Project Veritas Action Fund, 285 F.Supp.3d 109, 120 (D.D.C. 2018). Under D.C. law, a breach of a fiduciary duty "require[s] a showing of injury or damages." Headfirst Baseball LLC v. Elwood, 239 F.Supp.3d 7, 14 (D.D.C. 2017); see also Randolph, 973 A.2d at 709.

e. Statutory claims

[12] **[13]** Under the Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-408(a), a plaintiff must "plead actual injury or harm," Lloyd v. Gen. Motors Corp., 397 Md. 108, 916 A.2d 257, 277 (2007) (citing Citaramanis v. Hallowell, 328 Md. 142, 613 A.2d 964, 969 (1992)). "[T]o

articulate a cognizable injury under the [Maryland] Consumer Protection Act, the injury must be objectively identifiable," meaning "the consumer must have suffered an identifiable loss, measured by the amount the consumer spent or loss as a result of his or her reliance on the sellers' misrepresentation." Id.

[14] The Virginia Consumer Protection Act also requires a plaintiff to plead actual loss in order to bring a suit for damages under the Act. See ***11** Polk v. Crown Auto, Inc., 228 F.3d 541, 543 (4th Cir. 2000) (citing Va. Code Ann. § 59.1-204(A)); see also Chisolm v. TranSouth Fin. Corp., 194 F.R.D. 538, 549 (E.D. Va. 2000).

Finally, by its terms, the District of Columbia Data Breach Notification Act likewise requires "actual damages," which do "not include dignitary damages, including pain and suffering." D.C. Code Ann. § 28-3853(a).

2. Four theories of actual damages

The Court discerns four possible theories of actual damages in plaintiffs' complaint and briefing: (1) actual and/or heightened risk of misuse of personal information, (2) loss of the "benefit of the bargain" they struck when they purchased their policies, (3) consequential damages like expenditures credit monitoring services, and (4) emotional distress. The Court will address each theory in turn.

a. Misuse of personal information

[15] **[16]** The first theory of damages may be the most obvious in the context of a data breach: actual or heightened risk of misuse of exposed personal information. Plaintiffs generally allege that they have suffered both an "increased risk of identity theft, and also actual identity theft and resulting losses." SAC ¶ 17. They continue, "[m]any Plaintiffs and Class Members suffered from actual economic injury resulting in tax-refund fraud, identity theft, credit card fraud, and other conduct causing direct economic injury as a result of the identity theft they suffered." Id. ¶ 20; see also id. ¶ 58 ("many Plaintiffs have already suffered from direct economic injury such as tax-refund fraud, identity theft, [and] credit card fraud.").

The rub, though, is that only two of the named plaintiffs —the Tringlers from Maryland—actually allege that they have already experienced any kind of economic injury. The Tringlers contend that they "*have* experienced tax-refund fraud" as a result of the breach. Id. ¶ 57 (emphasis added). [4] The rest claim only the threat of misuse by listing what "identity thieves" "*can* " or "*may* " do with the kind of personal information accessed. See id. ¶¶ 49–51, 55 (emphases added). But the District of Columbia Court of Appeals has expressly declined to treat an increased risk of future identity theft as an actual harm for purposes of negligence and breach of fiduciary duty claims based on data breaches. See Randolph, 973 A.2d at 708–09. [5] And there is no reason to believe that court would decide any differently if presented with plaintiffs' other causes of action that require actual harm.

Plaintiffs do not confront the substance of this binding decision of the District of Columbia Court of Appeals head on. Instead, they incorrectly describe Randolph as a case about "the law of standing." Opp'n at 10 n.4. Although the lower court did conclude that the Randolph plaintiffs lacked standing, the D.C. Court of Appeals clearly explained that "the better approach toward resolving [the] motion to dismiss is to analyze whether the amended complaint ***12** succeeded in stating a claim." Randolph, 973 A.2d at 707.

Accordingly, with respect to plaintiffs' negligence and breach of fiduciary duty claims, the Court is bound by the Randolph decision. And, because this Court sitting in diversity is charged with determining how the D.C. Court of Appeals would rule in the absence of a case directly on point, the Court concludes that the D.C. Court of Appeals would likely hold, consistent with Randolph, that the mere threat of misuse of personal information would not be sufficient to state a claim for actual damages under the remaining seven claims not addressed in that decision. Thus, under District of Columbia law, only the Tringlers have alleged actual damages under this first theory of damages—misuse of exposed personal information.

b. Benefit of the bargain theory of damages

[17] Plaintiffs also contend that they were harmed by "a loss of the benefit of the bargain." Opp'n at 5–6. Under this theory, plaintiffs allege that they "provided payment to Defendants for certain services, including health insurance coverage, part of which was intended to pay administrative costs of securing their [sensitive personal information]." SAC ¶ 25. In return, however, they "received services devoid of

these very important protections." Id. ¶ 26. In other words, plaintiffs allege that they overpaid for their health insurance because they contracted for a service that would include data security but received a service that did not. This "benefit of the bargain" loss is, plaintiffs say, "the standard measure" of damages in breach of contract claims. Opp'n at 8.

District of Columbia courts have not addressed whether a "benefit-of-the-bargain" or "overpayment" theory of damages is sufficient to state a claim for actual damages in the data-breach context. But two fellow courts in this district have addressed the theory when considering 12(b)(1) motions to dismiss for lack of standing, and both rejected it as too "indeterminate." In In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litigation, 45 F.Supp.3d 14 (D.D.C. 2014) ("SAIC"), for example, Judge Boasberg rejected the data-breach plaintiffs' argument that they plausibly alleged "actual loss" by "claim[ing] that some indeterminate part of their premiums went toward paying for security measures." Id. at 30. He explained that the plaintiffs had not alleged that the money paid could have gone towards a better data-security policy or "that the market value of their insurance coverage (plus security services) was somehow less than what they paid." Id.; see also Austin-Spearman v. AARP & AARP Servs. Inc., 119 F.Supp.3d 1, 13–14 (D.D.C. 2015) (K.B. Jackson, J.) (concluding that plaintiff failed to plausibly plead economic injury-in-fact based on an "overpayment" theory—that is, that she paid for an online membership that included particular data-security benefits but received one that did not (citing SAIC, 45 F.Supp.3d at 30)). [6]

***13** As is often the case in the data-breach context, there are courts that disagree. The Eighth Circuit, for example, has held that a plaintiff plausibly alleged an injury-in-fact for standing based on a "devaluation" of his video-game subscription "in an amount equal to the difference between the value of the subscription that he paid for and the value of the subscription that he received, *i.e.*, a subscription with compromised privacy protection." Carlsen, 833 F.3d at 909. And Judge Koh in the Northern District of California has generally embraced the benefit-of-the-bargain theory when considering 12(b)(6) motions in data-breach cases. See In re Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F.Supp.3d 1113, 1130 (N.D. Cal. 2018) (concluding that plaintiff's "allegations are sufficient to allege that he suffered benefit-of-the-bargain losses" because he "pleads that he has paid $ 19.95 each year since December 2007 for Yahoo's premium email service," which was supposed to be "secure," and he would not have signed up "had he known that Yahoo's email service was not as secure as [Yahoo] represented"); In re Anthem, Inc. Data Breach Litig., 162 F.Supp.3d 953, 992, 995 (N.D. Cal. 2016) (adopting "loss of benefit of the bargain" theory of "actual harm" for New York plaintiffs who alleged they had contracted for "reasonable and adequate security measures" that Anthem failed to deliver, causing plaintiffs to overpay for their health insurance); In re Anthem, Inc. Data Breach Litig., No. 15-md-2617, 2016 WL 3029783, at *12–13 (N.D. Cal. May 27, 2016) (concluding same for California plaintiffs' breach-of-contract claim, which required "appreciable and actual" damages).

At the hearing, plaintiffs argued that "there has been a definite trend" away from the conclusion in cases like SAIC and towards those in cases like Anthem and Yahoo!. Hr'g Tr. at 35:2–35:6. But trend or no across the country, the Court declines to go beyond the decisions of its fellow courts in cases like SAIC and Austin-Spearman in the absence of controlling law from the District of Columbia Court of Appeals, especially because the standard for alleging actual damages is generally higher than that for plausibly alleging an injury-in-fact. Moreover, as in SAIC, plaintiffs here broadly allege that some indeterminate amount of their health insurance premiums went towards providing data security. SAC ¶ 25. And as in SAIC, they allege only in conclusory fashion that the services they received "were of a diminished value." Id. ¶ 73. This distinguishes the allegations here from those in In re Yahoo!, for example, where the plaintiffs put a number—the $ 19.95 subscription fee for a premium email service with allegedly better security—on the value of the contracted-for data security. Accordingly, the Court concludes that plaintiffs fail to state a claim for actual damages under their benefit-of-the-bargain theory.

c. "Mitigation costs" theory of damages

[18] Plaintiffs devote much of their opposition brief to a third theory of damages, this one related to their efforts to protect against identity theft. They allege that they "have or will have to spend significant time and money to protect themselves." SAC ¶ 19. These costs include "the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, cost of conducting a damage assessment, mitigation costs, costs to rehabilitate [their sensitive information], and costs to reimburse from losses incurred as a proximate result of the breach." Id. It is unclear whether plaintiffs contend that this category of "mitigation" costs constitutes economic damage in its own

right or is recoverable as consequential damages. Compare SAC ¶ 17 (Plaintiffs "need to take immediate action to protect themselves from identity theft, which have already ***14** and will continue to result in real and actual loss regardless of whether identity theft actually occurs."); Opp'n at 5 (describing "the loss of money and time in the form of expenditures made to protect themselves" as "actual economic damage"); Hr'g Tr. at 45:17 (describing "loss mitigation" as "direct economic harm"), with Opp'n at 7 ("Plaintiffs have alleged that as a consequence of Defendants' failures, breaches and misrepresentations, they have lost time and money."); id. at 8 ("[P]laintiffs who allege a breach of contract may recover both consequential and incidental damages.").

The District of Columbia Court of Appeals has rejected the theory that prophylactic mitigation measures constitute actual damages in their own right. In Randolph, the court explained that no plaintiff had alleged any misuse of any personal information that had been compromised by the theft of a company laptop containing personal information. 973 A.2d at 708. The court then addressed the plaintiffs' alternative argument regarding preventative expenditures:

> [T]o the extent [the plaintiffs] allege actual harm from expenses they have incurred to undertake credit monitoring or other security measures to guard against possible misuse of their data, they have alleged an injury that is 'not the result of any present injury, but rather the [result of] the anticipation of future injury that has not materialized.'

973 A.2d at 708 (citation omitted) (third alteration in original). Because "the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury the law [of negligence] is prepared to remedy," id. (alteration in original) (quoting Shafran v. Harley-Davidson, No. 07-cv-1365, 2008 WL 763177, at *3 (S.D.N.Y. Mar. 24, 2008)), the court concluded that the plaintiffs had failed to state a negligence claim. The court dismissed the plaintiffs' common-law breach of fiduciary duty claim "[f]or much the same reason." Id. at 709.[7] Under Randolph, then, time and money spent protecting against future identity theft cannot constitute damage in their own right for purposes of plaintiffs' negligence and breach of fiduciary duty claims.[8] And again, there is no reason to believe the D.C. Court of Appeals would treat plaintiffs' other D.C. law claims any differently.

This is consistent with how the vast majority of courts have treated mitigation costs in the context of data-breach litigation. They have distinguished between plaintiffs whose information has been exposed *and* misused and those whose information has been exposed but not misused. These courts draw the line at responsive versus preventative expenditures. For the former, costs are generally recoverable as ***15** consequential damages; for the latter, costs are not actual damages in their own right and cannot be recovered as consequential damages because there is not an actual injury, only an anticipated one.

For example, in Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007), the Seventh Circuit considered whether Indiana contract and tort law would permit recovery for the cost of "past and future credit monitoring services" incurred by bank customers after a hacker accessed their confidential information on the bank's website. Id. at 631, 635. "Significantly, the plaintiffs did not allege any *completed direct* financial loss to their accounts.... [n]or did they claim that they ... *already had been* the victim of identity theft[.]" Id. at 632. The court concluded that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy" by expending time and resources to monitor and protect their identities. Id. at 639; see also, e.g., Hendricks v. DSW Shoe Warehouse, Inc., 444 F.Supp.2d 775, 783 (W.D. Mich. 2006) (rejecting "plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss," which would have been "a novel legal theory of damages" for a breach of contract in Michigan, "based on a risk of injury at some indefinite time in the future"); Forbes v. Wells Fargo Bank, N.A., 420 F.Supp.2d 1018, 1020–21 (D. Minn. 2006) (rejecting plaintiffs' contention for both negligence and breach-of-contract claims "that the time and money they have spent monitoring their credit suffices to establish damages" in "anticipation of future injury that has not materialized").

Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018), on which plaintiffs rely, see Opp'n at 7, is not to the contrary. In that case, a class of plaintiffs sued Barnes & Noble after discovering that hackers had accessed individuals' names and credit card information on the company's computer system. Dieffenbach, 887 F.3d at 827. A named plaintiff from California alleged four kinds of injury stemming from the data breach after someone used her account "to make a fraudulent purchase": a delay in the restoration of funds to her bank account, the time she spent coordinating with

the police and her bank, a delay in her ability to use the compromised account, and her failure to receive the full measure of her bargain with Barnes & Noble. Id. at 828–29. The Seventh Circuit concluded that the first three losses were actual economic injuries sufficient to state a claim. Id. at 829. [9] The same was true for the named plaintiff from Illinois, who decided to renew her monthly credit-monitoring service after her bank contacted her about a potentially fraudulent charge and froze her card for several days. Id. In other words, the Seventh Circuit considered credit-monitoring and other mitigation services to be cognizable injuries for both named plaintiffs *who alleged they were already experiencing actual misuse*. See also Anthem, 2016 WL 3029783, at *15–16 (describing these kind of mitigation costs as "consequential out of pocket expenses" where plaintiff was notified his personal information was stolen, he learned that his financial information had been "compromised" and "used for unauthorized charges," and *then* he "took actions to prevent further financial damage").

***16** Apart from the Tringlers, plaintiffs here complain only of the cost of prophylactic, rather than responsive, measures. Consistent with the weight of authority on this issue, the remaining plaintiffs who have not alleged actual misuse of their exposed personal information may not plead actual damages under a mitigation-cost theory. Only the Tringlers —who, as discussed above, have alleged actual misuse in the form of tax-refund fraud—would be able to recover consequential damages like the money spent monitoring their credit.

d. Emotional distress

[19] Finally, plaintiffs seek non-economic damages for five of the nine claims that require actual damage: negligence, SAC ¶ 83; negligence *per se*, id. ¶ 129; violation of the Maryland Consumer Protection Act ("MCPA"), id. ¶ 109; fraud, id. ¶ 122; and constructive fraud, id. ¶ 152. [10] They claim that, in addition to economic loss, they have suffered "non-economic loss in the form of mental and emotional pain and suffering and aguish [sic] as a result of Defendants' failures." Id. ¶ 38. Based on the Court's conclusions regarding plaintiffs' theories of economic loss, all but the Tringlers are left with allegations of purely emotional damages. At the hearing, CareFirst took the position that emotional distress alone may as a matter of law sustain a claim for actual damages, but that here, plaintiffs have failed to adequately plead emotional distress. Hr'g Tr. at 15:24–16:15. The Court sees two questions: first, whether a plaintiff may sustain a claim for negligence, fraud, or violation of the MCPA based solely on emotional distress; and second, whether plaintiffs have adequately pled such damages here.

[20] The District of Columbia Court of Appeals applies "a different framework" for "[c]laims of negligence that seek damages for only mental pain and suffering." Hedgepeth v. Whitman Walker Clinic, 22 A.3d 789, 795 (D.C. 2011). To state a claim where "emotional distress is the only injury suffered," id. at 810, the plaintiff must satisfy either the "zone of physical danger" rule set out in Williams v. Baker, 572 A.2d 1062 (D.C. 1990) (en banc), or the special relationship and undertaking rule set out in Hedgepeth, 22 A.3d at 810–11. Such "negligent infliction of emotional distress" claims are distinct from other negligence claims where the plaintiff seeks to recover for pain and suffering as "parasitic" damages as a result of or incident to the "invasion of another legally protected interest." Hedgepeth, 22 A.3d at 809.

Plaintiffs' allegations regarding their pain and suffering are too conclusory to satisfy either the Williams or Hedgepeth rule. See Hawkins v. Wash. Metro. Area Transit Auth., 311 F.Supp.3d 94, 107–08 (D.D.C. 2018) (dismissing negligent infliction of emotional distress claim where plaintiffs failed to plead "serious and verifiable" emotional distress). This makes sense: Plaintiffs did not set out to state a claim only for emotional damages. Rather, they seek "ancillary or 'parasitic' damages for related mental distress (sometimes referred to as 'pain and suffering')." Hedgepeth, 22 A.3d at 795. As such, they cannot sustain their negligence and negligence *per se* claims based on emotional distress alone.

The same is true for plaintiffs' fraud and constructive fraud claims. Although a ***17** plaintiff may seek both economic and emotional damages in an action for intentional fraud, Osbourne v. Capital City Mort. Corp., 667 A.2d 1321, 1328 (D.C. 1995), superseded by statute on other grounds, D.C. Code Ann. § 28-3905(k)(1), the "*sine qua non* of any recovery for misrepresentation is a showing of pecuniary loss proximately caused by reliance on the misrepresentation," Kitt, 742 A.2d at 861 (quoting Day v. Avery, 548 F.2d 1018, 1029 (D.C. Cir. 1976) (per curiam)). Put another way, the economic torts of fraud and constructive fraud require some showing of economic harm in order for the plaintiff to recover emotional damages as well.

And finally, the Maryland Court of Appeals has held that the MCPA permits " 'recovery of damages for emotional

distress if there [is] at least a 'consequential' physical injury,' " but not where the plaintiff makes allegations like, "This made me feel bad; this upset me." Sager v. Hous. Comm'n of Anne Arundel Cty., 855 F.Supp.2d 524, 548–49 (D.Md. 2012) (quoting Hoffman v. Stamper, 385 Md. 1, 867 A.2d 276, 296 (2005)). Plaintiffs' allegations are more akin to the latter than the former, and thus cannot support a claim for a violation of the MCPA based on emotional distress alone.

Accordingly, plaintiffs' allegations of emotional distress are not sufficient to sustain their claims for negligence or negligence *per se*, fraud or constructive fraud, or violation of the MCPA.

* * *

Based on the foregoing, the Court will dismiss the following claims: breach of contract, negligence, negligence *per se*, fraud, constructive fraud, and breach of the duty of confidentiality brought by all plaintiffs but the Tringlers. The Court will also dismiss the District of Columbia Breach Notification Statute claim brought on behalf of the D.C. plaintiffs and the Virginia Consumer Protection Act claim brought on behalf of the Virginia plaintiffs. Finally, the Court will dismiss the Maryland Consumer Protection Act claim brought by Ms. Huber but not by the Tringlers. This leaves (at this point) the Tringlers with all of their claims; the D.C. plaintiffs with their unjust enrichment and D.C. Consumer Protection Procedures Act claims; the Virginia plaintiffs with their unjust enrichment claim; and Ms. Huber with her unjust enrichment claim. The Court now moves to the interplay between plaintiffs' contract and tort claims.

B. Whether the parties' contractual relationship bars plaintiffs' tort claims

[21] As an alternative to its arguments that plaintiffs fail to plead damages, CareFirst moves to dismiss plaintiffs' five tort claims—negligence, negligence *per se*, fraud, constructive fraud, and breach of a duty of confidentiality—based on the parties' contractual relationship. CareFirst asserts that plaintiffs cannot recover in tort for breach of duties that merely restate CareFirst's alleged contractual duties. According to CareFirst, because plaintiffs have failed to allege an independent common-law duty to reasonably safeguard personal information separate from any contractual one, they cannot "double dip" with claims sounding in tort. And even if there is such a duty, CareFirst asserts that the "economic loss rule" bars recovery here because, in the absence of a "special relationship" between parties, plaintiffs may not recover purely economic loses in tort. Finally, CareFirst contends that insurers and insureds do not have a fiduciary relationship that would support plaintiffs' claim for breach of a duty of confidentiality.

The Court starts and stops with the independent duty rule. Because the Court concludes that plaintiffs have failed to allege a duty to reasonably safeguard insureds' ***18** data separate from CareFirst's contractual duties—in part because the parties do not have a fiduciary relationship—it need not reach whether the parties are in a special relationship such that the economic loss rule would not apply.

[22] **[23]** "The failure to perform a contractual obligation typically does not give rise to a cause of action in tort." Jones v. Hartford Life & Accident Ins. Co., 443 F.Supp.2d 3, 5 (D.D.C. 2006). Under D.C. law, for a plaintiff to recover in tort for conduct that also constitutes a breach of contract, "the tort must exist in its own right independent of the contract, and any duty upon which the tort is based must flow from considerations other than the contractual relationship." Choharis v. State Farm Fire & Cas. Co., 961 A.2d 1080, 1089 (D.C. 2008). Thus, the viability of plaintiffs' tort claims turns on whether plaintiffs have plausibly alleged that CareFirst owes them an independent duty of care to reasonably safeguard private information beyond the parties' contractual relationship.

They have not. The complaint alleges no "facts separable from the terms of the contract upon which the tort may independently rest" and identifies no "duty independent of that arising out of the contract itself." Id. Plaintiffs assert that they "contracted for services that included a promise by Defendants to safeguard, protect, and not disclosure [sic] their personal information...." SAC ¶ 26; id. ¶ 66. They identify four sources of this promise: two CareFirst privacy policies, id. ¶¶ 28, 29, 67; its written services contract, which "promised" that CareFirst would "only disclose health information when required to do so by federal or state law," id. ¶ 66; and its "promise[ ] to comply with all HIPAA standards," id. ¶ 68. Plaintiffs' breach-of-contract claim turns on CareFirst's alleged breach of these promises. Id. ¶¶ 34, 72. Plaintiffs' negligence claim does not include additional facts or identify a separate duty to safeguard personal data; instead, it simply alleges that CareFirst "owed the Plaintiffs a duty of care in protecting the confidentiality of the personal and private information that the Plaintiffs provided to the Defendants as consumers of the Defendants' health insurance policies." Id. ¶ 77. This

allegation makes clear that "the duty of which [plaintiffs] essentially complain[ ]"—the duty to reasonably safeguard insureds' personal information—"necessarily arose from the contractual relationship." Nugent v. Unum Life Ins. Co. of Am., 752 F.Supp.2d 46, 54 (D.D.C. 2010). But for the contract between CareFirst and plaintiffs, CareFirst would not have had access to plaintiffs' information and thus would have had no occasion—or obligation—to protect it. [11]

Plaintiffs' response to Choharis is two-fold and doubly unsuccessful. First, they misinterpret its holding as being limited to a particular kind of tort—a first-party bad faith cause of action. See Opp'n at 17. The ***19** Choharis court clearly applied the broad rule—that "the tort must exist in its own right independent of the contract"—beyond the tort of bad faith to fraud and negligent misrepresentation as well. 961 A.2d at 1089–90 (affirming summary judgment where plaintiff's "assertions [regarding "fraudulent or negligent misrepresentation"] directly related to an obligation arising under the contract"). Plaintiffs' second argument implicitly reveals the error of their narrow interpretation of the case by attempting to fit their allegations into the Choharis framework: They contend that they have in fact alleged an "independent injury over and above the mere disappointment of plaintiff's hope to receive his contracted-for-benefit" because they do not allege that any "health insurance benefits were wrongfully denied." Opp'n at 17–18 (quoting Choharis, 961 A.2d at 1089). Put differently, they attempt —for purposes of their tort claims—to limit the contract's reach to the mere provision of health insurance benefits. But that argument undermines their contractual one—namely, that they "contracted for services that included a guarantee by Defendant to safeguard their personal information." SAC ¶ 21. Plaintiffs cannot have their cake (a contract that sets forth specific promises to safeguard information) and eat it too (a contract that provides only for the provision of health insurance). [12] Plaintiffs therefore fail to satisfy the Choharis requirement that they allege a tort duty independent of CareFirst's contractual obligations. [13]

***20** Even where plaintiffs fail to identify a non-contractual duty, some courts outside this jurisdiction have recognized a stand-alone duty to provide reasonable data security separate from any operative agreement. The District of Columbia Court of Appeals has not confronted this question. And jurisdictions across the country are divided as to whether there is a common law duty to provide data security. The courts that have recognized such a duty have rooted it in one, or a combination, of three theories: an affirmative duty to refrain from causing others harm, the foreseeability of harm, or the nature of the parties' relationship. The Court considers these theories in turn.

First, some courts have recognized a duty to provide reasonable data security under the "basic principle" of tort law that "everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm." In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F.Supp.2d 942, 966 (S.D. Cal. 2014) (quoting Yakubowicz v. Paramount Pictures Corp., 404 Mass. 624, 536 N.E.2d 1067, 1070 (Mass. 1989)). The Sony court concluded that this general duty to *refrain* translated to a specific "legal duty to *provide* reasonable network security ... separate and independent from the PSN User Agreement" and any contractual obligations that arose from that agreement. Id. at 968 (emphasis added). Because Sony allegedly breached that duty by "fail[ing] to employ reasonable security measures to protect" the plaintiffs' personal information—"provided ... to Sony as part of a commercial transaction"—the plaintiffs could "pursue both contract and tort remedies, to the extent [their] tort claims are not barred by the economic loss doctrine." Id. [14]

The Court is not persuaded by Sony's reasoning because it elides the distinction between a duty to refrain and a duty to act. While there may be a general duty to refrain from acts that cause others harm, this usually does not extend to an obligation to act affirmatively. Here, as in Sony, plaintiffs allege that CareFirst *failed* to act by not employing reasonable security measures to protect customers' personal information. The Court hesitates to recognize a common-law duty based on that alleged omission. See also Veridian Credit Union v. Eddie Bauer, LLC, 295 F.Supp.3d 1140, 1158 (W.D. Wash. 2017) (finding no common law duty to reasonably secure credit card information where plaintiffs' "allegations comprise numerous omissions or nonfeasance on the part of Eddie Bauer, but they do not describe misfeasance or any affirmative act 'that created a situation of peril' for [plaintiffs]" (citation omitted)).

[24] **[25]** Still, there are some circumstances under District of Columbia law where even a failure to act will give rise to a legal duty. "[W]hether a duty exists is the result of a variety of considerations." Bd. of Tr. of Univ. of Dist. of Columbia v. DiSalvo, 974 A.2d 868, 871 (D.C. 2009). These considerations include the foreseeability of harm and the nature of the relationship between the parties. ***21** Id. at 871–72 & 871 n.2; see also Hedgepeth, 22 A.3d at 794

("We have described a court's examination of whether a duty exists as a 'foreseeability of harm test' that is determined, in large part, by the nature of the relationship between the parties.") (quoting Odemns v. District of Columbia, 930 A.2d 137, 143 (D.C. 2007)). The balance of these considerations operates on "a sliding scale: If the relationship between the parties strongly suggests a duty of protection, then specific evidence of foreseeability is less important, whereas if the relationship is not of a type that entails a duty of protection, then the evidentiary hurdle is higher." DiSalvo, 974 A.2d at 872 (quoting Workman v. United Methodist Comm. on Relief, 320 F.3d 259, 264 (D.C. Cir. 2003)).

This leads to the second theory: Some of the courts that have recognized a common law duty to reasonably secure consumers' data have done so based on the foreseeability of harm. For example, in In re Arby's Restaurant Group, Inc. Litigation, No. 1:17-cv-514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018), a group of financial institutions and consumers sued Arby's after hackers breached the restaurant's point of sales machines. Id. at *1. Applying Georgia law, the court emphasized the role that "foreseeability" plays "in defining the existence of a legal duty." Id. at *3. More specifically, the Arby's court explained that under state law, a person or entity "may still have a duty to protect against a criminal act of a third person," which would include hacking into a private data system, "if it is alleged that [the entity] had 'reason to anticipate' the criminal act." Id. (citation omitted). In that case, the plaintiffs alleged that Arby's knew or should have known about the risk of a data breach based on known problems specific to Arby's point of sales system as well as other recent highly publicized data breaches in that industry. Id. at *5. The court found those allegations "sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss." Id.; id. at *12 (concluding that both tort and contract actions could proceed because plaintiffs identified "a common law duty that would have applied regardless of the existence of an underlying contract"). [15] Here, by contrast, plaintiffs have made no allegations that it was foreseeable that CareFirst specifically would suffer a data breach based on, for instance, known vulnerabilities in its data-storage systems.

And third, some courts that have recognized a common law duty in the data-breach context have done so based on the nature of the relationship between the party providing the confidential information and the party receiving it, as well as the sensitive nature of the information provided. An inquiry into the nature of the relationship often overlaps with two separate but related legal questions: whether the "special relationship" exception to the economic loss rule barring tort claims applies and whether there is a fiduciary relationship to support a duty of confidentiality. In some cases, the analysis merges entirely.

Take Daly v. Metropolitan Life Insurance Co., 4 Misc.3d 887, 782 N.Y.S.2d 530 (N.Y. Sup. Ct. 2004), where a New York trial court considered "a new area of law"—namely, "whether liability may attach to an entity that fails to safeguard personal and confidential information obtained in conjunction with the purchase of a life insurance policy." Id. at 532. In the ***22** absence of case law on this then-nascent legal question, the court drew a parallel to the breach of a fiduciary duty of confidentiality, where one party puts its trust in the other by relying on the other's superior expertise. Id. at 534–35. The court analogized that the insurance company—like a fiduciary—"had a duty to protect the confidential personal information provided by" subscribers because insurance subscribers were "required to" provide the insurance company "with highly sensitive personal information" in order to obtain life insurance and that company had represented in its privacy notice that it would safeguard that information. Id. at 535. At least one federal district court has adopted Daly's reasoning. In Jones v. Commerce Bancorp, Inc., the court concluded that a bank customer sufficiently alleged a legal duty to safeguard information where the bank required her to provide confidential personal information in order to open a business account and warranted that it would safeguard that information. No. 06-cv-835-HB, 2006 WL 1409492, at *1–2 (S.D.N.Y. May 23, 2006) (citing Daly, 782 N.Y.S.2d at 532–35).

The problems of data breaches may no longer be "new" but courts around the country continue to confront these legal questions. Just recently, for example, the Pennsylvania Supreme Court held for the first time 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." Dittman v. UPMC, —— Pa. ——, 196 A.3d 1036, 1038 (2018). The court rooted this duty in the traditional common law duty to exercise reasonable care when engaging in affirmative conduct as well as the nature of the relationship between the parties. The employees alleged that "as a condition of their employment," their employer "required them to provide certain personal and financial information, which [it] collected and stored on its internet-accessible computer system without use of adequate security measures."

Id. at 1047. According to the court, this dynamic was sufficient to allege a duty of care. Id.

Not all courts, however, have concluded that requiring another to provide sensitive personal information creates such a duty. For example, in Cooney v. Chicago Public Schools, 407 Ill.App.3d 358, 347 Ill.Dec. 733, 943 N.E.2d 23 (2010), the Appellate Court of Illinois concluded that Chicago Public Schools did not owe a legal duty to safeguard its employees' personal information. Id., 347 Ill.Dec. 733, 943 N.E.2d at 29. In that case, the Chicago Board of Education inadvertently disclosed the personal information, including social security numbers and health insurance plan information, of almost 2,000 former employees. Id. 347 Ill.Dec. 733, 943 N.E.2d at 27. The employees urged the court to "recognize a 'new common law duty' to safeguard information" in light of the sensitive nature of personal data that was disclosed and the fact that the Board had collected that data. Id. 347 Ill.Dec. 733, 943 N.E.2d at 28–29. But the Illinois court declined to go beyond state statutory notice requirements and recognize a new duty in the absence of specific authority. Id. 347 Ill.Dec. 733, 943 N.E.2d at 29. "Federal courts interpreting Illinois law have consistently declined to impose a common law duty to safeguard personal information in data security cases" based on Cooney. In re SuperValu, Inc., Customer Data Sec. Breach Litig., 14-md-2586-ADM-TNL, 2018 WL 1189327, *14 (D. Minn. Mar. 7, 2018). In SuperValu, for instance, consumers argued that SuperValu owed them "an extra-contractual duty" because it "solicited customers' [private personal information] and thus had a duty to take reasonable measures to safeguard their data and notify them of any data breach." Id. The district court declined to recognize such a duty. Id.; see also, e.g., ***23** Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 816 (7th Cir. 2018) (relying on Cooney to conclude that Illinois "would not impose the common law data security duty the plaintiff banks call for here"); Gordon, 2018 WL 3653173, at *15 (citing Cooney and Community Bank of Trenton to dismiss an Illinois negligence claim "for lack of a common law duty").

[26] **[27]** Because the District of Columbia Court of Appeals has not determined one way or the other whether there is a common law duty to safeguard data, the Court will follow the approach taken in some of the cases cited above and look to analogous case law regarding the nature of the relationship between insurers and insureds. "District of Columbia law does not ... consider the relationship between insurer and insured a fiduciary relationship" as a matter of law. Gebretsadike v. Travelers Home & Marine Ins. Co., 103 F.Supp.3d 78, 83 (D.D.C. 2015) (citing Fireman's Fund Ins. Co. v. CTIA-The Wireless Ass'n, 480 F.Supp.2d 7, 15 (D.D.C. 2007)); see also Stevens v. United Gen. Title Ins. Co., 801 A.2d 61, 66 (D.C. 2002) (applying contract rather than fiduciary principles to determine whether duty to defend exists). This is consistent with other jurisdictions. Instead, the relationship between parties to an insurance contract is generally considered "contractual in nature." See Fero, 236 F.Supp.3d at 773-74 (quoting Batas v. Prudential Ins. Co. of Am., 281 A.D. 2d 260, 264, 724 N.Y.S.2d 3 (N.Y. Sup. Ct. 2001)) (declining to recognize a "special relationship" necessary for negligent misrepresentation claim between health insurance provider and consumers whose confidential health information was accessed), withdrawn on other grounds by 304 F.Supp.3d 333 (W.D.N.Y. 2018); In re Premera Blue Cross Customer Data Sec. Breach Litig., 198 F.Supp.3d 1183, 1203 (D. Or. 2016) ("[T]he nature of the relationship between the parties [consumers and their insurance company] is not the type of relationship that historically has been considered fiduciary in character."); Dolmage v. Combined Ins. Co. of Am., No. 14-cv-3809, 2015 WL 292947, at *6 (N.D. Ill. Jan. 21, 2015) ("In Illinois, it is well settled that no fiduciary relationship exists between an insurer and an insured as a matter of law." (internal alterations, quotation marks, citation omitted)).

Plaintiffs try to avoid this precedent by reframing their relationship with CareFirst as a doctor-patient one, which has been historically recognized as a fiduciary relationship as a matter of law. See Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 591–92 (D.C. 1985). They allege—for purposes of their breach of the duty of confidentiality claim *only*—that CareFirst owed them such a duty "pursuant to its fiduciary relationship with the Plaintiffs ... as their *health care providers*." SAC ¶ 139 (emphasis added). But CareFist obviously is not a provider of healthcare; it is a provider of health care *insurance*, as plaintiffs repeatedly acknowledge elsewhere throughout their complaint. See, e.g., SAC ¶ 23 ("Defendants are a network of for-profit *health insurers* which provide *health insurance coverage* to individuals[.] (emphases added)"); see also id. ¶¶ 25, 60, 65, 77, 89, 125. Accordingly, no doctor-patient relationship exists that would give rise to a duty of confidentiality as a matter of law.

[28] **[29]** Even where, as here, a fiduciary relationship does not exist as a matter of law, District of Columbia courts may imply such a relationship in special circumstances. Determining whether a fiduciary relationship exists requires "a searching inquiry into the nature of the relationship, the

promises made, the types of services or advice given and the legitimate expectations of the parties." Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz, 793 F.Supp.2d 311, 341 (D.D.C. 2011) (quoting ***24** Firestone v. Firestone, 76 F.3d 1205, 1211 (D.C. Cir. 1996)); Church of Scientology Int'l v. Eli Lilly & Co., 848 F.Supp. 1018, 1028 (D.D.C. 1994) (recognizing that even though "no Court has ever found there to be a fiduciary relationship between a public relations firm and one of its clients," the court faced a "fact-intensive question" about "the nature of the relationship" specific to the parties before it). In addition, "a fiduciary relationship could exist [ ] where circumstances show that the parties extended their relationship beyond the limits of the contractual obligations to a relationship founded upon trust and confidence." Paul v. Judicial Watch, Inc., 543 F.Supp.2d 1, 6 (D.D.C. 2008) (citing Church of Scientology, 848 F.Supp. at 1028); see also Ying Qing Lu v. Lezell, 919 F.Supp.2d 1, 6 (D.D.C. 2013) ("While fiduciary relationships can be difficult to define, and may very well exist between contracting parties, '[o]ne characteristic that District of Columbia courts have traditionally looked for is a "special confidential relationship" that transcends an ordinary business transaction and requires each party to act with the interests of the other in mind.' " (citing High v. McLean Fin. Corp., 659 F.Supp. 1561, 1568 (D.D.C. 1987))).

Plaintiffs fail to plead anything to suggest that their relationship with CareFirst was anything more than the typical commercial relationship between insurer and insureds. As in Fero, nothing about the alleged "interactions would appear to fall outside the scope of what is routine between insurers and insureds, and therefore, the interactions do no suggest any kind of special relationship of trust and confidence." 236 F.Supp.3d at 773–74. True, CareFirst required plaintiffs to provide personal and confidential information, but this will be the case in almost every insurer-insured relationship. Plaintiffs do not allege a relationship beyond that envisioned in every day interactions with a health insurance provider that would give rise to either a common law duty to safeguard private information or a fiduciary duty. As such, negligence, negligence *per se*, and breach of the duty of confidentiality are misplaced legal theories on which to pursue recovery for the data breach.

[30] The same is true for plaintiffs' fraud and constructive fraud claims, which likewise arise out of the same alleged conduct that supports their breach of contract claim. "District of Columbia law requires that the factual basis for a fraud claim be separate from any breach of contract claim that may be asserted." Plesha v. Ferguson, 725 F.Supp.2d 106, 113 (D.D.C. 2010) (citing Choharis, 961 A.2d at 1089). The plaintiffs in Plesha failed to satisfy this requirement because their allegations of fraud arose out of the same alleged conduct by defendants—"late payments and promises to pay"—that provided the basis for their breach of contract claim. Id. So too here. For their contract claim, plaintiffs allege that CareFirst breached its "promise[ ] through its Internet Privacy Policy that it would encrypt all personal information given to Defendants." SAC ¶¶ 67, 72. For their fraud claim, plaintiffs similarly allege that CareFirst "made false representations of material facts" in its "Internet Privacy Policy and General Privacy Policy, which indicated that information provided ... would be encrypted." Id. ¶ 118; see also id. ¶ 150 (alleging, for constructive fraud claim, that CareFirst owed plaintiffs a duty "to abide by the privacy policies it had incorporated and to safeguard personal health information"). CareFirst's allegedly unfulfilled promise to encrypt all personal information thus cannot constitute a separately actionable fraud or constructive fraud claim.

* * *

Based on the foregoing, the Court will dismiss all plaintiffs' tort claims, including negligence, negligence *per se*, breach of the duty of confidentiality, fraud, and constructive ***25** fraud. This leaves the following: the Tringlers with their breach of contract, unjust enrichment, and Maryland Consumer Protection Act claims; Ms. Huber of Maryland with her unjust enrichment claim; the D.C. plaintiffs with their unjust enrichment and D.C. Consumer Protection Procedures Act claims; and the Virginia plaintiffs with their unjust enrichment claim. The Court turns next to unjust enrichment.

C. Whether plaintiffs have pled in the alternative an unjust enrichment claim

[31] **[32]** **[33]** CareFirst contends that its undisputed contractual relationship with plaintiffs also precludes their unjust enrichment claim. MTD at 15–16. It is well-established that the existence of a valid contract precludes a claim for unjust enrichment. See, e.g., Harrington v. Trotman, 983 A.2d 342, 346 (D.C. 2009) (holding that superior court "fundamentally erred as a matter of law in finding unjust enrichment when there was a valid contract between the parties"). Plaintiffs counter that while they cannot ultimately recover under both theories, they may plead unjust enrichment in the alternative should the Court later find no contractual agreement between the parties. Opp'n at 18–19. True enough, courts "sometimes permit[ ] a party

to plead [unjust enrichment] as an alternative in certain circumstances." He Depu v. Yahoo! Inc., 306 F.Supp.3d 181, 193–94 (D.D.C. 2018) (citation omitted). But the devil is in the details: Such an alternative theory "require[s] an allegation that the contract is invalid and unenforceable." Id. Plaintiffs have not alleged this, and CareFirst confirmed at the hearing that it has not taken the position that the contract is invalid or unenforceable. See Sony, 996 F.Supp.2d at 984–85, 984 n.37 (dismissing unjust enrichment claims, pled in the alternative, where plaintiffs did not challenge validity or enforceability of user agreements); Hr'g Tr. 20:5–20:11.

Accordingly, the Court will dismiss the unjust enrichment claim for all plaintiffs. This leaves unaddressed the D.C. Consumer Protection Procedures Act claim brought on behalf of the D.C. plaintiffs and the Maryland Consumer Protection Act claim brought on behalf of the Tringlers. [16]

D. Whether plaintiffs have alleged an unlawful trade practice under the D.C. Consumer Protection Procedures Act

Like their tort claims, the District of Columbia plaintiffs' D.C. Consumer Protection Procedures Act ("DCCPPA") claim is premised on CareFirst's alleged breach of its contractual obligations. They allege that CareFirst "violated [its] Internet Privacy Policy" and thus "committed and [sic] unfair and unlawful trade practice" by not providing the benefits provided for in that policy and misrepresenting a material fact "as indicated in their Internet Privacy Policy." SAC ¶ 88. [17]

The Court can interpret plaintiffs' DCCPPA allegations in one of two ways, ***26** neither of which passes muster. On the one hand, plaintiffs could be alleging that the mere breach of contract constitutes an unlawful trade practice under the DCCPPA. But they cite no support for this proposition and at least one court in this district has implied that a DCCPPA claim must be premised on at least *some* additional conduct other than a run-of-the-mill breach. See Jacobson v. Hofgard, 168 F.Supp.3d 187, 199–200, 206–07 (D.D.C. 2016) (denying motion to dismiss because DCCPPA claim was not "inappropriately duplicative of Plaintiffs' breach of contract claim" where alleged misrepresentation preceded the formation of the contract); see also Am. Airlines, Inc. v. Wolens, 513 U.S. 219, 233, 115 S.Ct. 817, 130 L.Ed.2d 715 (1995) (concluding, under Illinois law, that "a breach of contract, without more, 'does not amount to a cause of action cognizable under the Consumer Fraud Act and the Act should not apply to simply breach of contract claims" (internal alterations, quotation marks, citation omitted)).

[34] On the other hand, plaintiffs could be alleging that CareFirst "misrepresented a material fact"—which would constitute an unlawful trade practice under the DCCPPA—by stating that it would comply with the terms of its Internet Privacy Policy knowing full well that it would not. But another court in this district has concluded that under D.C. law, "an intentional breach of contract"—which is essentially what plaintiffs would need to argue under this misrepresentation theory—"is not punishable as an unlawful trade practice under the Consumer Protection Procedures Act simply because the breach was intended when the contract was formed." Slinski v. Bank of Am., N.A., 981 F.Supp.2d 19, 36 (D.D.C. 2013). The Court agrees with that reasoning.

Accordingly, because the D.C. plaintiffs' DCCPPA claim is entirely duplicative of their breach of contract claim and an intentional breach of contract cannot constitute an unlawful trade practice, the Court will dismiss this claim as well.

E. Whether insurance companies are exempt from civil liability for data breaches under the Maryland Consumer Protection Act

[35] Last but not least, the Court addresses CareFirst's argument that all of the plaintiffs' claims under the Maryland Consumer Protection Act ("MCPA")—including the Tringlers'—must be dismissed because the Act exempts insurance companies from liability. MTD at 19–20. The MCPA expressly states that its provisions do not apply to the "professional services" of an "insurance company." Md. Code Ann., Com. Law § 13-104(1). The question then is whether "professional services" as that term is used under the Act applies to the data-security services at issue in this case.

Maryland's highest court has interpreted "professional services" narrowly as applied to "medical or dental practitioner[s]," who are also exempt under the MCPA. In Scull v. Groover, Christie & Merritt, P.C., 435 Md. 112, 76 A.3d 1186 (2013), the Maryland Court of Appeals held that a radiology office's medical-billing practices were not exempt under the professional-services exemption because those practices were related to the "commercial or entrepreneurial" aspects of the office rather than the "actual rendering of health care services." Id. at 1196, 1197–98. [18] To reach ***27** this conclusion, the court considered the statutory function of the state's Consumer Protection Division's ("CPD") Health

Education and Advocacy Unit, which is authorized to refer disputes regarding a medical provider's billing practices, but not the adequacy of its treatment, to the CPD for potential enforcement actions, as well as the CPD's longstanding view that the MCPA applies to medical-billing practices. Id. at 1194–95. The court also considered the legislative history of another exemption directed specifically at health care services. Id. at 1194. Finally, the court identified other areas of the law that distinguish between the ancillary services of a medical office like billing and the more direct services like treating a wound or implanting a dental filling. For example, professionals are generally licensed based on specialized training and expertise directly related to their profession. Id. at 1195–96. And for negligence actions, a professional is generally held to a special standard of care applicable to their particular profession. Id.

The Court concludes that the professional-services exemption of the MCPA does not apply to CareFirst's data-security practices. Rather, gathering and storing consumers' private information is ancillary to the provision of health insurance coverage much like billing is ancillary to the provision of medical care. Other areas of Maryland law reinforce the conclusion that an insurance company's data-security practices are not exempt as a professional service. Maryland's Personal Information Protection Act provides that "a business that owns or licenses personal information of an individual" must "implement and maintain reasonable security procedures and practices" in order to "protect personal information from unauthorized access, use, modification, or disclosure." Md. Code Ann., Com. Law § 14-3503. Under the Act, "business" is defined broadly to include any "business entity," and "personal information" is defined broadly to include data like a person's name combined with their social security number, credit card number, or health information. Id. § 14-3501(b)(1) & (e)(1). Health information is in turn defined as "any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996" ("HIPAA"). Id. § 14-3501(d). As a health insurance provider covered by HIPAA, CareFirst appears to be subject to the Personal Information Protection Act. And because consumers may bring a violation of that Act as an unfair or deceptive trade practice under the MCPA, id. § 14-3508, exempting CareFirst's data-security services from the MCPA would create an inconsistency in state law similar to the one the Scull court tried to avoid.

Therefore, the Court will deny CareFirst's motion to dismiss the Tringlers' Maryland Consumer Protection Act claim.

V. Conclusion

For the foregoing reasons, Defendants' motion to dismiss will be granted in part and denied in part. The Court will grant the motion to dismiss for all but the Tringlers' breach of contract claim in Count I and the Maryland Consumer Protection Act claim in Count V. A separate order accompanies this memorandum opinion.

All Citations

365 F.Supp.3d 1

Footnotes

1 The named plaintiffs are Chantal Attias and Andreas Kotzur of the District of Columbia, Richard and Latanya Bailey of Virginia, and Curt and Connie Tringler and Lisa Huber of Maryland. Id. ¶¶ 1–4.

2 Although there was some confusion in the briefing, the parties agreed at the hearing that District of Columbia law applies to all but the state-specific statutory claims. See Opp'n at 12; Hr'g Tr. at 6:2–6:10.

3 See also Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016) ("As we previously have cautioned, [i]t is crucial ... not to conflate Article III's requirement of injury in fact with a plaintiff's potential causes of action, for the concepts are not coextensive." (internal quotation marks and citation omitted) (alterations in original)).

4 While the Tringlers have not alleged specific facts connecting the two events, the Court must draw all reasonable inferences in favor of plaintiffs when considering a motion under Rule 12(b)(6). Accordingly, even though the Tringlers may ultimately fail to prove causation at summary judgment, it can be plausibly inferred for present purposes.

5 Randolph is not an outlier. Other courts across the country have likewise distinguished between plaintiffs whose data has been exposed *and* misused and those whose data has been exposed but not misused for purposes of claims requiring actual damages. See, e.g., Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.").

6 Courts in other jurisdictions have likewise concluded that alleged overpayment for health insurance that does not include bargained-for data security is not sufficient to allege injury-in-fact for purposes of standing. See Fero v. Excellus Health Plain, Inc., 236 F.Supp.3d 735, 754–55 (W.D.N.Y. 2017) (listing cases). In Chambliss v. CareFirst, Inc., 189 F.Supp.3d 564 (D. Md. 2016), the Maryland class action arising out of the same CareFirst data breach, the court rejected the plaintiffs' benefit-of-the-bargain theory of injury in finding a lack of standing. The court explained, "Plaintiffs make no allegations that the data breach diminished the value of the health insurance they purchased from CareFirst" nor do they offer "factual allegations indicating that the prices they paid for health insurance included a sum to be used for data security." Id. at 572. As a result, the Chambliss plaintiffs did not "quantify this alleged loss." Id. So too here.

7 Cf. In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., 266 F.Supp.3d 1, 40 (D.D.C. 2017), appeal filed No. 18-1182 (dismissing case for lack of subject matter jurisdiction where plaintiffs failed to allege facts that would support waiver of sovereign immunity under Privacy Act because "those plaintiffs who purchased credit monitoring services or incurred other expenses to prevent future identity theft have not suffered actual damages because expenditures undertaken voluntarily to prevent possible future harm do not constitute actual damages" (citation omitted)).

8 The D.C. Circuit concluded that plaintiffs plausibly alleged redressability for purposes of Article III standing because they "reasonably spent money to protect themselves against a substantial risk," meaning they could "be made whole by monetary damages." Attias, 865 F.3d at 629. But again, Article III standing and actual damages are separate questions governed by federal and state law respectively. Therefore, the preventative measures plaintiffs have taken may be sufficient to support redressability but are not, under D.C. law, sufficient as actual damages.

9 Hewing to the result in the majority of cases cited in Section (IV)(A)(2)(b) above, the Seventh Circuit rejected the argument that the plaintiff suffered an economic "benefit of the bargain" loss because she did not contend that any of the items she purchased were "defective" or that "Barnes & Noble promised any particular level of security, for which she paid." Id. at 829.

10 Plaintiffs do not seek emotional distress damages for their breach of contract, D.C. Data Breach Notification Statute, Virginia Consumer Protection Act, and breach of the duty of confidentiality claims. Id. ¶¶ 74, 97, 114, 144. In any event, emotional distress damages would not be recoverable for at least some of these claims. See Howard Univ. v. Baten, 632 A.2d 389, 392 (D.C. 1993) (breach of contract); D.C. Code ¶ 28-3853(a) (excluding "dignitary harms, including pain and suffering," from the definition of "[a]ctual damages" under the D.C. Data Breach Notification Statute).

11 Other federal courts across the country have dismissed data-breach negligence claims where the plaintiffs failed to identify a non-contractual duty to safeguard private information. See, e.g., Gordon v. Chipotle Mexican Grill, Inc., No. 17-cv-1415-CMA-MLC, 2018 WL 3653173, at *16–17 (D. Colo. Aug. 1, 2018), magistrate R & R adopted in relevant part by 344 F.Supp.3d 1231, 1246-47 (D. Colo. 2018) (dismissing negligence claim in consumer data breach case where "[p]laintiffs do not cite any Colorado authorities to support [the assertion that] Defendant had an independent duty to safeguard [private information]" and plaintiffs "alleged the same duty under their implied contract"); SELCO Cmty. Credit Union v. Noodles & Co., 267 F.Supp.3d 1288, 1295 (D. Colo. 2017) (dismissing financial-institution data breach case where plaintiffs "cite no support for the existence of specific common law or statutory duties of care related to data security" and "most important of all," the duties alleged by plaintiffs were "created by, and completely contained in, the contractual provisions" (citation omitted)).

12 Plaintiffs advanced a version of this argument at the hearing. When asked to explain where in the complaint they allege an independent duty, counsel responded that CareFirst's "privacy policy" constitutes "a separate representation" from the contractual representations that more obviously relate to health insurance, like a promise to "cover my claim if I hurt my leg." Hr'g Tr. at 42:11–42:18. But when the Court pointed out that plaintiffs also base their contract claim in part on the promises made in those policies, counsel simply responded, "[i]t's broken promises in the four corners of the contract, and it's broken promises outside of the four corners of the contract." Id. at 44:20–44:22. This response only reinforces the Court's conclusion that plaintiffs have not alleged an *independent* duty.

13 Responding to CareFirst's arguments regarding the economic loss rule, plaintiffs contend that "it has already been held that an insurer has 'additional obligations' beyond those stated in a contract by nature of the insurer-insured relationship." Opp'n at 15 (citing Cent. Armature Works, Inc. v. Am. Motorists Ins. Co., 520 F.Supp. 283, 292 (D.D.C. 1980)). Although it does not reach the economic loss rule arguments, the Court will address this contention to the extent it can be construed as asserting that such "additional obligations" give rise to some sort of independent duty. In Central Armature Works, the court upheld an award of punitive damages in a breach of contract action against an insurance company in part because "an insurer has additional obligations to its insured which subject it to more stringent standards of conduct than those normally imposed on parties to a contract." 520 F.Supp. at 292. Acknowledging that "[n]either party [ ] presented any authority from the District of Columbia which establishes the relationship between an insurer and its insured," id.,

the court relied on out-of-district precedent and a general assertion by the District of Columbia Court of Appeals that insurers have a "duty to process and pay claims expeditiously and in good faith," id. (quoting Cont'l Ins. Co. v. Lynham, 293 A.2d 481, 483 (D.C. 1972)). In 1993, the D.C. Circuit likewise relied on out-of-district precedent to explain that the "bad faith tort [for "refusal to pay insurance benefits"] is grounded on the covenant of good faith and fair dealing that is implicit in all contracts [and] supplemented by the idea that insurance contracts have special characteristics that warrant heightened liability for breach of that covenant." Messina v. Nationwide Mut. Ins. Co., 998 F.2d 2, 5 (D.C. Cir. 1993). But since Central Armature Works and Messina, "the D.C. Court of Appeals has spoken clearly and 'bad faith conduct,' to the extent proved, 'can be compensated within those principles' of the contractual obligation of good faith and fair dealing." Nugent, 752 F.Supp.2d at 56 (quoting Choharis, 961 A.2d at 1087). Coming full circle, then, plaintiffs' overreading of Central Armature Works to impose a separate *tort* as opposed to *contractual* obligation is foreclosed by Choharis.

14 Demonstrating the complicated interaction between the independent duty doctrine and the economic loss rule, the Sony court ultimately concluded that the "special relationship" exception to the economic loss rule did not apply because the plaintiffs "failed to allege a 'special relationship' with Sony beyond those envisioned in everyday consumer transactions." Id. at 969. "[T]herefore, negligence [was] the wrong legal theory on which to pursue recovery for [their] economic losses." Id.

15 See also, e.g., In re The Home Depot, Inc. Customer Data Sec. Breach Litig., No. 1:14-md-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."); In re Target Corp. Customer Data Sec. Breach Litig., 64 F.Supp.3d 1304, 1310 (D. Minn. 2014) (same).

16 Remember that the Court dismissed the MCPA claim brought on behalf of the other Maryland plaintiff, Ms. Huber, because she failed to allege actual damages.

17 Plaintiffs also alleged that CareFirst violated the DCCPPA by failing to comply with HIPAA. Originally, CareFirst moved to dismiss the DCCPPA claim (as well as the breach of contract, negligence, and negligence *per se* claims) as premised on an alleged violation of HIPAA, which does not have a private right of action. MTD at 16. Plaintiffs have since disavowed reliance on alleged HIPAA violations for all but their negligence *per se* claim. Opp'n at 19. Because the Court has already concluded that plaintiffs have not stated a claim for negligence *per se* due to their failure to allege actual damages and their failure to identify an independent duty, it need not address this alternative basis for dismissal.

18 CareFirst relies on outdated case law to argue that the professional-services exemption applies "broadly" even when one acts outside their professional capacity. MTD at 20 (citing Lembach v. Bierman, 528 F. App'x 297, 304 (4th Cir. 2013)). For this proposition, the Fourth Circuit in Lembach relied on the Maryland Court of Special Appeals' decision in Scull v. Doctors Groover, Christie & Merritt, P.C., 205 Md.App. 567, 45 A.3d 925 (Md. Ct. Spec. App. 2012). But the Fourth Circuit issued Lembach in June 2013, before Maryland's highest court reversed in relevant part the Court of Special Appeals' decision below. See Scull, 76 A.3d at 1196–97.

Senate Bill No. 1121

CHAPTER 735

An act to amend Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.185, 1798.192, 1798.196, and 1798.198 of, and to add Section 1798.199 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately.

[Approved by Governor September 23, 2018. Filed with Secretary of State September 23, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 1121, Dodd. California Consumer Privacy Act of 2018.

(1) Existing law, the California Consumer Privacy Act of 2018, grants, commencing on January 1, 2020, a consumer various rights with regard to personal information relating to that consumer that is held by a business, including the right to request a business to delete any personal information about the consumer collected by the business, and requires the business to comply with a verifiable consumer request to that effect, unless it is necessary for the business or service provider to maintain the customer's personal information in order to carry out specified acts. The act requires a business that collects personal information about a consumer to disclose the consumer's right to delete personal information described above on its Internet Web site or in its online privacy policy or policies.

This bill would modify that requirement by requiring a business that collects personal information about a consumer to disclose the consumer's right to delete personal information in a form that is reasonably accessible to consumers and in accordance with a specified process.

(2) The act establishes several exceptions to the requirements imposed, and rights granted, by the act, including prohibiting the act from being interpreted to restrict the ability of a business to comply with federal, state, or local laws, and by providing that the act does not apply if it is in conflict with the California Constitution.

This bill would provide that the rights afforded to consumers and the obligations imposed on any business under the act does not apply if those rights or obligations would infringe on the noncommercial activities of people and entities described in a specified provision of the California Constitution addressing activities related to newspapers and periodicals. The bill would also prohibit application of the act to personal information collected, processed, sold, or disclosed pursuant to a specified federal law relating to banks, brokerages, insurance companies, and credit reporting agencies, among others, and would also except application of the act to that information pursuant to the California Financial Information Privacy Act.

The bill would provide that these exceptions, and the exception provided to information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994, do not apply to specific provisions of the act related to unauthorized theft and disclosure of information. The bill would revise and expand the exception provided for medical information, would except a provider of health care or a covered entity, and would also except information collected as part of clinical trials, as specified. The bill would also clarify that the act does not apply if it is in conflict with the United States Constitution.

(3) The act generally provides for its enforcement by the Attorney General, but also provides for a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information, as defined for this purpose, provided that the consumer bringing an action notify the Attorney General of the action in accordance with a specified process. The act provides that a business, service provider, or other person who violates its provisions, and fails to cure those violations within 30 days, is liable for a civil penalty under laws relating to unfair competition in an action to be brought by the Attorney General. The act prescribes a formula for allocating civil penalties and settlements assessed in these actions with 80% to be allocated to the jurisdictions of the behalf of which the action was brought.

This bill would clarify that the only private right of action permitted under the act is the private right of action described above for violations of unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information and would delete the requirement that a consumer bringing a private right of action notify the Attorney General. The bill would remove references to laws relating to unfair competition in connection with Attorney General actions described above. The bill would limit the civil penalty to be assessed in an Attorney General action in this context to not more than $2,500 per violation or $7,500 per each intentional violation and would specify that an injunction is also available as remedy. The bill would eliminate the formula for allocating penalties and settlements and would instead provide that all of these moneys be deposited in the Consumer Privacy Fund with the intent to offset costs incurred by the courts and the Attorney General in connection with the act. The bill would also revise timelines and requirements regarding the promulgation of regulations by the Attorney General in connection with the act.

(4) The act makes its provisions operative on January 1, 2020, provided a specified contingency is satisfied. Provisions of the act supersede and preempt laws adopted by local entities regarding the collection and sale of a consumer's personal information by a business.

This bill would make the provisions of the act that supersede and preempt laws adopted by local entities, as described above, operative on the date the bill becomes effective.

(5) This bill would also make various technical and clarifying changes to the act.

(6) This bill would declare that it is to take effect immediately as an urgency statute.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.100 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.100. (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

SEC. 2. Section 1798.105 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal

information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

SEC. 3. Section 1798.110 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.110. (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

SEC. 4. Section 1798.115 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.115. (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

SEC. 5. Section 1798.120 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

SEC. 6. Section 1798.125 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

SEC. 7. Section 1798.130 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.130. (a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the

consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

SEC. 8. Section 1798.135 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this

section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

SEC. 9. Section 1798.140 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.140. For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated

for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service,

processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(*l*) "Homepage" means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Not be used for any commercial purpose.

(9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing

consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

SEC. 10. Section 1798.145 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that

personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of “medical information” and “provider of health care” in Section 56.05 shall apply and the definitions of “business associate,” “covered entity,” and “protected health information” in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial

Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(k) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

SEC. 11. Section 1798.150 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.150. (a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of

subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

SEC. 12. Section 1798.155 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.155. (a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged

noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

SEC. 13. Section 1798.185 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.185. (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood

by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

SEC. 14. Section 1798.192 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.192. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

SEC. 15. Section 1798.196 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.196. This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

SEC. 16. Section 1798.198 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.198. (a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

SEC. 17. Section 1798.199 is added to the Civil Code, to read:

1798.199. Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

SEC. 18. This act is an urgency statute necessary for the immediate preservation of the public peace, health, or safety within the meaning of Article IV of the California Constitution and shall go into immediate effect. The facts constituting the necessity are:

In order to prevent the confusion created by the enactment of conflicting local laws regarding the collection and sale of personal information, it is necessary that this act take immediate effect.

O

KeyCite Yellow Flag - Negative Treatment
Disagreed With by Dieffenbach v. Barnes & Noble, Inc., 7th Cir.(Ill.), April 11, 2018

407 Ill.App.3d 358
Appellate Court of Illinois,
First District, Sixth Division.

Jacqueline COONEY, Emma Martin, Michele Hardin, Gwendolyn Jones, Karen Soprych, Thomas Balek, Robert Giancarlo and Eulett Cox, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs–Appellants,
v.
CHICAGO PUBLIC SCHOOLS; The Board of Education of the City of Chicago; and All Printing and Graphics, Inc., Defendants–Appellees.
Jan Morgan–Wulf; Allison Padelford and Paul Rieger et al., Indiv. and on Behalf of All Persons and Entities Similarly Situated, Plaintiffs–Appellants,
v.
The Board Of Education of the City of Chicago and All Printing and Graphics, Inc., Defendants–Appellees.

No. 1–09–1215.
|
Dec. 30, 2010.

Synopsis

Background: After city board of education accidentally disclosed the personal information of former school employees in a mailing designed to inform them of their health insurance choices, former employees brought consolidated actions against board and against printing company that prepared and sent the mailing on board's behalf. The Circuit Court, Cook County, Rita Novak, J., granted board's and printing company's motions to dismiss. Former employees appealed.

Holdings: The Appellate Court, Cahill, J., held that:

[1] board's accidental disclosure did not violate Health Insurance Portability and Accountability Act of 1996 (HIPAA);

[2] Personal Information Protection Act did not establish the existence of a duty sufficient to support a negligence action;

[3] board had no common law duty to safeguard former employees' personal information;

[4] printing company had no duty to protect the former employees' information from disclosure;

[5] board owed no fiduciary duty to former employees;

[6] former employees failed to allege actual damages, as necessary to support a claim under the Consumer Fraud Act; and

[7] former employees' social security numbers were not "private facts," so as to give rise to an invasion of privacy claim.

Affirmed.

Robert E. Gordon, J., filed dissenting opinion.

West Headnotes (24)

[1] **Appeal and Error** De novo review
Appeal and Error Pleading

Appellate Court reviews de novo a dismissal with respect to the pleadings and a dismissal based on certain defects or defenses. S.H.A. 735 ILCS 5/2–615, 5/2–619.

[2] **Pretrial Procedure** Availability of relief under any state of facts provable

A complaint is properly dismissed with respect to the pleadings where there is no set of facts that if proven would entitle the plaintiff to recovery. S.H.A. 735 ILCS 5/2–615.

[3] **Pretrial Procedure** Affirmative Defenses, Raising by Motion to Dismiss

A complaint is properly dismissed based on certain defects or defenses where no genuine

issue of material fact exists and the defendant is entitled to judgment as a matter of law. S.H.A. 735 ILCS 5/2–619.

[4] **Negligence** Elements in general

To succeed on a negligence claim, plaintiffs must allege and prove that: (1) defendants owed a duty to plaintiffs; (2) defendants breached that duty; and (3) the breach caused injury to plaintiffs.

9 Cases that cite this headnote

[5] **Education** Other particular injuries to persons other than students or teachers

Privileged Communications and Confidentiality Employment relationships; personnel records

Records Exemptions or prohibitions under other laws

City board of education's accidental disclosure of personal information belonging to former school employees, in a mailing designed to inform them of their health insurance choices, did not violate Health Insurance Portability and Accountability Act of 1996 (HIPAA), and thus HIPAA did not create a duty owed to the former employees sufficient to support a negligence claim against board; employment records held by an employer were exempted from HIPAA protection. Health Insurance Portability and Accountability Act of 1996, § 262(a), 42 U.S.C.A. § 1320d–6(a)(3); 45 C.F.R. § 160.103.

2 Cases that cite this headnote

[6] **Negligence** Necessity and Existence of Duty

Where no duty is owed, there is no negligence.

6 Cases that cite this headnote

[7] **Negligence** Violations of statutes and other regulations

Negligence Violations of statutes and other regulations

A violation of a statute designed to protect human life and property may be used as prima facie evidence of negligence.

1 Cases that cite this headnote

[8] **Antitrust and Trade Regulation** Privacy

Personal Information Protection Act, which required a data collector to promptly notify the owner of personal information of any security breach, did not establish the existence of a duty sufficient to support a negligence action by former school employees against city board of education arising out of board's accidental disclosure of their personal information to other former employees; only obligation imposed by the Act in the event of a breach of security was notification, which board complied with. S.H.A. 815 ILCS 530/5, 530/10(b).

5 Cases that cite this headnote

[9] **Education** Other particular injuries to persons other than students or teachers

City board of education had no common law duty to safeguard the personal information of former school employees, and thus its accidental disclosure of such information, in a mailing designed to inform the former employees of their health insurance choices, did not give rise to a negligence action.

14 Cases that cite this headnote

[10] **Negligence** Necessity and Existence of Duty

Negligence Contractual duty

Printing company that printed and sent a mailing on behalf of city board of education that contained the personal information of former school employees had no duty to protect the former employees' information from disclosure and, thus, was not liable to the former employees for negligence; printing company met its contractual obligations by printing and mailing the board's information packets, and was not required to inspect the contents of the mailing or inform the board of any irregularities.

3 Cases that cite this headnote

[11] **Damages** Negligent Infliction of Emotional Distress

A plaintiff claiming to be a direct victim of negligently inflicted emotional distress must establish the traditional elements of negligence: (1) duty; (2) breach; (3) causation; and (4) injury.

9 Cases that cite this headnote

[12] **Fraud** Fiduciary or confidential relations

City board of education owed no fiduciary duty to former school employees, as necessary to support a claim for breach of fiduciary duty arising out of board's accidental disclosure of the former employees' personal information.

1 Cases that cite this headnote

[13] **Fraud** Fiduciary or confidential relations

To state a cause of action for a breach of a fiduciary relationship, a plaintiff must allege that the defendant owed a fiduciary duty to the plaintiff, and that duty must exist as a matter of law.

5 Cases that cite this headnote

[14] **Civil Rights** Governmental Ordinance, Policy, Practice, or Custom

To establish municipal liability under § 1983, a plaintiff must allege that he has been deprived of a constitutionally protected right and that deprivation was caused by a municipal policy, custom or practice. 42 U.S.C.A. § 1983.

2 Cases that cite this headnote

[15] **Civil Rights** Governmental Ordinance, Policy, Practice, or Custom

A plaintiff may establish municipal liability under § 1983 by showing: (1) an express policy that causes a constitutional deprivation when enforced; (2) a widespread practice that is so permanent and well-settled that it constitutes a custom or practice; or (3) an allegation that the constitutional injury was caused by a person with final policymaking authority. 42 U.S.C.A. § 1983.

2 Cases that cite this headnote

[16] **Civil Rights** Cooperation with state actor

Non-state actors may be found liable under § 1983 where they have conspired or acted in concert with state actors to deprive a person of his civil rights. 42 U.S.C.A. § 1983.

[17] **Appeal and Error** Particular Cases and Contexts

Former school employees forfeited, for purposes of appeal, their claim that city board of education's accidental disclosure of their personal information violated the Fourth Amendment, even though issue was mentioned in amended complaint, where issue was never briefed or argued before the trial court, and was completely ignored by the trial court. U.S.C.A. Const.Amend. 4.

[18] **Antitrust and Trade Regulation** Persons and Transactions Covered Under General Statutes

City board of education could not be held liable under the Consumer Fraud Act for accidentally disclosing the personal information of former school employees; Act only barred such disclosure by a "person," which included business entities but did not include political bodies. S.H.A. 815 ILCS 505/1(c); 815 ILCS 505/2QQ(a)(1) (2006 Bar Ed.)

[19] **Antitrust and Trade Regulation** Privacy

Former school employees failed to allege actual damages resulting from the accidental disclosure of their personal information in a mailing from city board of education, as necessary to support a claim under the Consumer Fraud Act against printing company that prepared and sent the mailing on board's behalf; increased risk of

future identity theft was not actual harm, and purchase of credit monitoring services was not an economic injury. S.H.A. 815 ILCS 505/1(c), 505/10a(a); 815 ILCS 505/2QQ(a)(1) (2006 Bar Ed.)

10 Cases that cite this headnote

[20] **Antitrust and Trade Regulation** Reliance; causation; injury, loss, or damage

To support a Consumer Fraud Act claim, actual damages must arise from purely economic injuries. S.H.A. 815 ILCS 505/10a(a).

10 Cases that cite this headnote

[21] **Torts** Types of invasions or wrongs recognized

Illinois recognizes four ways to state a cause of action for invasion of privacy: (1) intrusion upon the seclusion of another; (2) appropriation of another's name or likeness; (3) public disclosure of private facts; and (4) publicity placing another in a false light.

10 Cases that cite this headnote

[22] **Torts** Intrusion

To support an invasion of privacy claim based on the theory of intrusion upon the seclusion of another, plaintiffs must allege: (1) an unauthorized intrusion into seclusion; (2) the intrusion would be highly offensive to a reasonable person; (3) the matter intruded upon was private; and (4) the intrusion caused the plaintiffs anguish and suffering.

18 Cases that cite this headnote

[23] **Torts** Publications or Communications in General

An invasion of privacy claim based on public disclosure of private facts requires that: (1) publicity was given to the disclosure of private facts; (2) the facts were private, and not public, facts; and (3) the matter made public was such as to be highly offensive to a reasonable person.

15 Cases that cite this headnote

[24] **Torts** Particular cases in general

Torts Miscellaneous particular cases

Former school employees' social security numbers were not "private facts," and thus city school board's accidental disclosure of those numbers did not give rise to an invasion of privacy claim, based on either intrusion into the seclusion of another or public disclosure of private facts, even though Personal Information Protection Act defined social security numbers as personal information; private facts were distinct from personal information, and consisted of facts that were facially embarrassing and highly offensive if disclosed. S.H.A. 815 ILCS 530/5.

15 Cases that cite this headnote

Attorneys and Law Firms

****26** Keith L. Hunt, Hunt & Associates, P.C., Chicago, for Appellants.

Mare N. Blumenthal, Law Office of Marc N. Blumenthal, Chicago, for the Morgan–Wulf Appellants.

Rick J. Rocks, William A. Morgan, Lisa D. Hugé, Board of Education of the City of Chicago, Chicago, for Appellee Board of Education of the City of Chicago.

Karen L. Kendall, Heyl Royster, Voelker & Allen, Peoria; Marion Victoria Cruz, James D. Montgomery & Associates, Ltd., Chicago, for Appellee All Printing & Graphics, Inc.

Opinion

****27** Justice CAHILL delivered the opinion of the court:

*****737** ***360** Plaintiffs appeal the circuit court's order dismissing claims stemming from disclosure of the personal information of approximately 1,700 former Chicago Public School (CPS) employees. We affirm.

Defendant All Printing & Graphics, Inc., was retained by the Board of Education of the City of Chicago (Board) to print, package and mail a "Chicago Public Schools–COBRA

Open Enrollment List" to over 1,700 former CPS employees. The mailing, sent sometime between November 23, 2006, and November 27, 2006, informed the former employees that as COBRA participants, they could change their insurance benefit plans. The list sent to each plaintiff contained the names of all 1,750 plaintiffs, along with their addresses, social security numbers, marital status, medical and dental insurers and health insurance plan information (COBRA list).

On November 26, 2006, the Board learned of the disclosure of the personal information. The following day the Board sent a letter to the former employees, asking them to return the COBRA list or destroy it.

***361** On December 8, 2006, the Board mailed the former employees a letter offering one year of free credit protection insurance.

Some of the former employees filed individual and class action lawsuits, and the cases were later consolidated. The complaints allege: (1) violation of the Personal Information Protection Act (the Act) (815 ILCS 530/1 *et seq.* (West 2006)); (2) violation of the Consumer Fraud and Deceptive Business Practices Act (Consumer Fraud Act) (815 ILCS 505/1 *et seq.* (West 2006)); (3) violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. 1320d–6 (2006)) under 42 U.S.C. § 1983; (4) violation of the common law right to privacy; (5) violation of the Illinois Constitution's privacy clause (Ill. Const.1970, art. I, § 6); (6) negligent infliction of emotional distress; (7) negligence; and (8) breach of fiduciary duty. Defendants moved to dismiss the complaints under sections 2–615 and 2–619 of the Illinois Code of Civil Procedure (735 ILCS 5/2–615, 2–619 (West 2006)). The trial court dismissed the complaints with prejudice.

Plaintiffs appeal the dismissal of all claims with the exception of the alleged violation of the Illinois Constitution's privacy clause.

[1] **[2]** **[3]** We review *de novo* a dismissal under sections 2–615 and 2–619 of the Code. *Solaia Technology, LLC v. Specialty Publishing Co.,* 221 Ill.2d 558, 578–79, 304 Ill.Dec. 369, 852 N.E.2d 825 (2006). A complaint is properly dismissed under section 2–615 of the Code where there is no set of facts that if proven would entitle the plaintiff to recovery. *Marshall v. Burger King Corp.,* 222 Ill.2d 422, 429, 305 Ill.Dec. 897, 856 N.E.2d 1048 (2006). A complaint is properly dismissed under section 2–619 of the Code where no genuine issue of material fact exists and the defendant is entitled to judgment as a matter of law. *Doyle v. Holy Cross Hospital,* 186 Ill.2d 104, 109–10, 237 Ill.Dec. 100, 708 N.E.2d 1140 (1999).

[4] Plaintiffs first argue that the trial court erred in dismissing their common law and statutory negligence claims. To succeed on their negligence claims, plaintiffs must allege and prove that (1) defendants owed a duty to plaintiffs; (2) defendants breached that duty; and (3) the breach caused injury to plaintiffs. *First Springfield Bank & Trust v. Galman,* 188 Ill.2d 252, 256, 242 Ill.Dec. 113, 720 N.E.2d 1068 (1999).

****28** *****738** **[5]** **[6]** **[7]** We must first decide whether the Board had a duty to safeguard plaintiffs' personal information under a statutory directive, because where no duty is owed, there is no negligence. *Washington v. City of Chicago,* 188 Ill.2d 235, 239, 242 Ill.Dec. 75, 720 N.E.2d 1030 (1999). Plaintiffs argue that HIPAA (42 U.S.C. § 1320d–6 (2006)) provides a statutory basis for the creation of a new duty. A violation of a statute designed to protect human life and property may be used as *prima facie* evidence of negligence. *Kalata v. Anheuser–Busch Cos.,* 144 Ill.2d 425, 434–35, 163 Ill.Dec. 502, 581 N.E.2d 656 (1991). HIPAA prohibits the disclosure of "individually ***362** identifiable health information to another person." 42 U.S.C. 1320d–6(a)(3) (2006). But, "employment records held by a covered entity in its role as employer" are specifically excluded from HIPAA protection. 45 C.F.R. § 160.103 (2006). Because the Board held plaintiffs' health insurance elections in its role as an employer, the Board's disclosure falls outside HIPAA's coverage.

Plaintiffs also contend that the Act (815 ILCS 530/1 *et seq.* (West 2006)) creates a legal duty. The Act provides:

> "Any data collector that maintains computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." 815 ILCS 530/10(b) (West 2006).

The " '[b]reach of the security of the system data' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information [including social security numbers] maintained by the data collector." 815 ILCS 530/5 (West

2006). In defining "data collector," the Act includes "government agencies * * * and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information." 815 ILCS 530/5 (West 2006).

[8] Plaintiffs claim that the Board, as a data collector, violated the Act because a "breach of the security of the system data" occurred. Plaintiffs are correct, but while the statute defines what a breach of system security is, it also codifies the remedy: the data collector must provide timely notice of a security breach to the parties affected. 815 ILCS 530/10 (West 2006). The Board complied with the statute by timely notifying plaintiffs of the breach.

Plaintiffs suggest that we adopt an expansive reading of the Act. The argument can be summarized as follows: in enacting the Act, the legislature intended to protect personal information from disclosure. If the only obligation imposed by the Act is to provide notice of a breach, its purpose would be defeated because entities could repeatedly disclose personal information and then exonerate themselves by providing notice. So, the statute's purpose can only be realized by penalizing the disclosure itself.

Because the provisions in the Act are clear, we must assume it reflects legislative intent to limit defendants' duty to providing notice. See *Comprehensive Community Solutions, Inc. v. Rockford School District No. 205,* 216 Ill.2d 455, 473, 297 Ill.Dec. 221, 837 N.E.2d 1 (2005) ("[t]he plain language of a statute remains the best indication of [the legislature's] intent").

[9] ***363** Plaintiffs next contend that we should recognize a "new common law duty" to safeguard information. They claim a duty is justified by the sensitivenature *****739** ****29** of personal data such as dates of birth and social security numbers. Plaintiffs do not cite to an Illinois case that supports this argument. While we do not minimize the importance of protecting this information, we do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review. As noted, the legislature has specifically addressed the issue and only required the Board to provide notice of the disclosure.

[10] All Printing also had no duty to protect plaintiffs' information from disclosure. All Printing met its contractual obligations by printing and mailing the Board's information packets. Plaintiffs cite to no authority for the proposition that All Printing had a duty to inspect the contents of the packets or inform the Board of any irregularity. Absent a duty, there is no negligence. *Washington,* 188 Ill.2d at 239, 242 Ill.Dec. 75, 720 N.E.2d 1030. We affirm the trial court's dismissal of plaintiffs' negligence claims.

[11] Plaintiffs next seek recovery for negligent infliction of emotional distress. A plaintiff claiming to be a direct victim of negligently inflicted emotional distress must establish the traditional elements of negligence: duty, breach, causation and injury. *Corgan v. Muehling,* 143 Ill.2d 296, 306, 158 Ill.Dec. 489, 574 N.E.2d 602 (1991). Because plaintiffs failed to establish a duty on the part of either defendant, their negligent infliction of emotional distress claim must fail with their general negligence claims.

[12] **[13]** Plaintiffs next assert that the Board, as their former employer, had a fiduciary duty to avoid disclosure of personal information. "To state a cause of action for a breach of a fiduciary relationship, a plaintiff must allege that the defendant owed a fiduciary duty to the plaintiff, and that duty must exist as a matter of law." *Dames & Moore v. Baxter & Woodman, Inc.,* 21 F.Supp.2d 817, 823 (N.D.Ill.1998), citing *Mid–America National Bank of Chicago v. First Savings & Loan Ass'n of South Holland,* 161 Ill.App.3d 531, 538, 113 Ill.Dec. 367, 515 N.E.2d 176 (1987). Plaintiffs' sole contention is that a fiduciary duty was created when they provided the Board with information "in confidence." Plaintiffs cite to no authority supporting such a duty. See *Eckiss v. McVaigh,* 261 Ill.App.3d 778, 786, 199 Ill.Dec. 637, 634 N.E.2d 476 (1994) ("[m]ere contentions without argument or citation of authority do not merit consideration on appeal"). We affirm the trial court's dismissal of this claim.

Next, plaintiffs contend that the trial court erred in dismissing their causes of action under 42 U.S.C. § 1983 for a violation of HIPAA (42 U.S.C. § 1320d–6 (2006)) and the fourth amendment to the United States Constitution (U.S. Const., amend. IV).

[14] **[15]** **[16]** ***364** To establish municipal liability under section 1983 of Title 42 of the United States Code (42 U.S.C. § 1983 (2006)), a plaintiff must allege that he has been deprived of a constitutionally protected right and that deprivation was caused by a municipal policy, custom or practice. *Waters v. City of Chicago,* 580 F.3d 575, 580 (7th Cir.2009), citing *Monell v. Department of Social Services,* 436 U.S. 658, 694, 98 S.Ct. 2018, 2037–38, 56 L.Ed.2d 611, 638 (1978); see also *Weimann v. County of Kane,* 150

Ill.App.3d 962, 965, 104 Ill.Dec. 110, 502 N.E.2d 373 (1986). "A plaintiff may establish municipal liability by showing '(1) an express policy that causes a constitutional deprivation when enforced; (2) a widespread practice that is so permanent and well-settled that it constitutes a custom or practice; or (3) an allegation that the constitutional injury was caused by a person ***740 **30 with final policymaking authority.' " *Waters,* 580 F.3d at 581, quoting *Estate of Sims ex rel. Sims v. County of Bureau,* 506 F.3d 509, 515 (7th Cir.2007). Non-state actors, such as All Printing here, may be found liable where they have conspired or acted in concert with state actors to deprive a person of his civil rights. *Pesek v. Marzullo,* 566 F.Supp.2d 834, 839 (N.D.Ill.2008) (mem.op.), citing *Adickes v. S.H. Kress & Co.,* 398 U.S. 144, 152, 90 S.Ct. 1598, 1605–06, 26 L.Ed.2d 142, 151 (1970).

Plaintiffs have not cited to a case that supports the assertion of these rights in the context of a private right of action under HIPAA. See *Bagent v. Blessing Care Corp.,* 363 Ill.App.3d 916, 919–20, 300 Ill.Dec. 471, 844 N.E.2d 469 (2006) ("[HIPAA] * * * does not support a private cause of action"), *overruled on other grounds,* 224 Ill.2d 154, 308 Ill.Dec. 782, 862 N.E.2d 985 (2007); *University of Colorado Hospital Authority v. Denver Publishing Co.,* 340 F.Supp.2d 1142, 1145 (D.Colo.2004) (finding HIPAA precludes "implication of a private right of action" and citing other federal decisions finding no private right of action under HIPAA); *Doe v. Board of Trustees of the University of Illinois,* 429 F.Supp.2d 930, 944 (N.D.Ill.2006) ("[e]very court to have considered the issue * * * has concluded that HIPAA does not authorize a private right of action"); see also *Gonzaga University v. Doe,* 536 U.S. 273, 284, 122 S.Ct. 2268, 2275–76, 153 L.Ed.2d 309, 321–22 (2002) ("a plaintiff suing under an implied right of action must still show that the statute manifests an intent 'to create not just a private *right,* but a private *remedy* ' ") (emphasis in original), quoting *Alexander v. Sandoval,* 532 U.S. 275, 286, 121 S.Ct. 1511, 1519, 149 L.Ed.2d 517, 528 (2001).

[17] We also find that plaintiffs have forfeited the appeal of their fourth amendment claim. Plaintiff Cooney mentioned the fourth amendment in her third amended complaint but never briefed or argued the issue before the trial court. The trial court "completely ignored" the fourth amendment claim because Cooney failed to bring it before the court. ***365** See *People v. Phipps,* 238 Ill.2d 54, 62, 342 Ill.Dec. 893, 933 N.E.2d 1186, 1191 (2010), citing *People v. Blair,* 215 Ill.2d 427, 443–44, 294 Ill.Dec. 654, 831 N.E.2d 604 (2005) (forfeiture applies to issues that could have been raised but were not).

We turn next to plaintiffs' claims under the Consumer Fraud Act. 815 ILCS 505/1 *et seq.* (West 2006). Section 2QQ of the Consumer Fraud Act provides that a "person" may not "[p]ublicly post or publicly display in any manner an individual's social security number." 815 ILCS 505/2QQ(a)(1) (West 2006) (renumbered as 505/2RR in West 2008). It defines "[to] 'publicly post' or 'publicly display' " as "to intentionally communicate or otherwise make available to the general public." 815 ILCS 505/2QQ(a)(1) (West 2006).

[18] The statute defines a "person" as "any natural person or his legal representative, partnership, corporation (domestic and foreign), company, trust, business entity or association, and [agents and representatives of these entities]." 815 ILCS 505/1(c) (West 2006). The Board, as a body politic, is not a "person" within the meaning of the Consumer Fraud Act and therefore cannot be held liable for a violation of the statute. *Board of Education v. A, C & S, Inc.,* 131 Ill.2d 428, 467–68, 137 Ill.Dec. 635, 546 N.E.2d 580 (1989).

[19] **[20]** Unlike the Board, All Printing is a domestic corporation and qualifies as a "person" within the meaning of the Consumer Fraud Act. See 815 ILCS 505/1(c) (West 2006). But, plaintiffs must allege actual damages to bring a Consumer ***741 **31 Fraud Act action. See 815 ILCS 505/10a(a) (West 2006) ("[a]ny person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person"); see *Morris v. Harvey Cycle & Camper, Inc.,* 392 Ill.App.3d 399, 402, 331 Ill.Dec. 819, 911 N.E.2d 1049 (2009) ("[t]he failure to allege specific, actual damages precludes a claim brought under the Consumer Fraud Act"). To support a Consumer Fraud Act claim, actual damages must arise from " purely economic injuries." *Morris,* 392 Ill.App.3d at 402, 331 Ill.Dec. 819, 911 N.E.2d 1049.

Plaintiffs contend that they alleged actual damages because the disclosure put them at increased risk of future identity theft. In *Yu v. International Business Machines Corp.,* 314 Ill.App.3d 892, 247 Ill.Dec. 841, 732 N.E.2d 1173 (2000), we held that allegations of potential harm arising from a software defect were insufficient to support a Consumer Fraud Act claim, justifying a section 2–615 dismissal. Without actual injury or damage, the plaintiff's claims "constitute[d] conjecture and speculation." *Yu,* 314 Ill.App.3d at 897, 247 Ill.Dec. 841, 732 N.E.2d 1173. See also *Williams*

v. Manchester, 228 Ill.2d 404, 425, 320 Ill.Dec. 784, 888 N.E.2d 1 (2008) ("as a matter of law, an increased risk of future harm is an *element of damages* that can be recovered for a present injury-it is *not* the injury itself") (emphasis in original); *Pisciotta v. Old National Bancorp,* 499 F.3d 629, 639 (7th Cir.2007) ***366** ("[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy"); *Morris,* 392 Ill.App.3d at 403, 331 Ill.Dec. 819, 911 N.E.2d 1049, citing *Xydakis v. Target, Inc.,* 333 F.Supp.2d 686, 688 (N.D.Ill.2004) ("[t]here is no cause of action under the Consumer Fraud Act when a plaintiff alleges only aggravation and not actual damages").

Plaintiffs also allege actual economic injury: the purchase by some plaintiffs of credit monitoring services. They claim that the Board's offer of credit monitoring services constitutes an admission of actual damages.

While neither party has directed us to Illinois authority addressing whether the purchase of credit monitoring services constitutes an economic injury under the Consumer Fraud Act, there is federal authority on this issue supporting the position that the purchase of these services, without more, is not an economic injury. See *Rowe v. UniCare Life & Health Insurance Co.,* No. 09 C 2286, 2010 WL 86391 (N.D.Ill. January 5, 2010) (finding the *provision* of credit monitoring services by the defendants "does not resolve the question of whether credit monitoring costs are actual damages" and finding that "the costs of credit monitoring services are not a present harm in and of themselves"); *Aliano v. Texas Roadhouse Holdings LLC,* No. 07 C 4108, 2008 WL 5397510 (N.D.Ill. December 23, 2008) (finding that the purchase of credit monitoring services does not constitute actual damages and citing district courts in Michigan, Minnesota, Ohio and New York in agreement); see also *Harris v. Wal–Mart Stores Inc.,* No. 07 C 02561, 2008 WL 5085132 (N.D.Ill. November 25, 2008) (rejecting claim for damages under the Credit and Debit Card Receipt Clarification Act of 2007, Pub.L. No. 110–241, 122 Stat. 1565 (2008) (codified at 15 U.S.C. § 1681) for the cost of credit monitoring services). We affirm the trial court's dismissal of plaintiffs' Consumer Fraud Act claims.

[21] Finally, we address plaintiffs' invasion of privacy claims. Illinois courts recognize four ways to state a cause of action for invasion of privacy: "(1) intrusion *****742 **32** upon the seclusion of another; (2) appropriation of another's name or likeness; (3) public disclosure of private facts; and (4) publicity placing another in a false light." *Busse v. Motorola, Inc.,* 351 Ill.App.3d 67, 71, 286 Ill.Dec. 320, 813 N.E.2d 1013 (2004). Plaintiffs allege facts to support the first and third theories: intrusion upon seclusion and public disclosure of private facts.

[22] **[23]** To support the intrusion theory, plaintiffs must allege: (1) an unauthorized intrusion into seclusion; (2) the intrusion would be highly offensive to a reasonable person; (3) the matter intruded upon was private; and (4) the intrusion caused the plaintiffs anguish and suffering. *Busse,* 351 Ill.App.3d at 71, 286 Ill.Dec. 320, 813 N.E.2d 1013. Public disclosure of private facts requires that "(1) publicity was given to the disclosure of private ***367** facts; (2) the facts were private, and not public, facts; and (3) the matter made public was such as to be highly offensive to a reasonable person." *Miller v. Motorola, Inc.,* 202 Ill.App.3d 976, 978, 148 Ill.Dec. 303, 560 N.E.2d 900 (1990), citing W. Prosser, Torts § 117 (5th ed. 1984). While the theories contain different elements, both the intrusion and public disclosure torts require "private" matters or facts.

In *Busse,* we suggested that "[i]n the absence of an Illinois law defining social security numbers as private information, we cannot say that defendants' use of this number fulfills the privacy element necessary to plead intrusion upon seclusion." *Busse,* 351 Ill.App.3d at 73, 286 Ill.Dec. 320, 813 N.E.2d 1013. We also noted that matters of public record such as names and dates of birth have not been held to be private facts. *Busse,* 351 Ill.App.3d at 72, 286 Ill.Dec. 320, 813 N.E.2d 1013, citing *Geisberger v. Willuhn,* 72 Ill.App.3d 435, 439, 28 Ill.Dec. 586, 390 N.E.2d 945 (1979).

[24] Plaintiffs contend that, after *Busse,* the legislature defined social security numbers as private facts, overruling that holding. They again rely on the Act, which includes social security numbers in its definition of "personal information." 815 ILCS 530/5 (West 2006). By equating "personal" with "private" information, plaintiffs ignore the distinction we relied on in *Busse.* See *Busse,* 351 Ill.App.3d at 72, 286 Ill.Dec. 320, 813 N.E.2d 1013 ("[h]ere, none of the 'personal' information furnished by the customers * * * has been held to be private facts"). The language of the Act is consistent with *Busse,* which distinguished personal information, such as names and social security numbers, from private facts, which are facially embarrassing and highly offensive if disclosed. See 815 ILCS 530/5 (West 2006); *Busse,* 351 Ill.App.3d at 72–73, 286 Ill.Dec. 320, 813 N.E.2d 1013, comparing *Johnson v. K mart Corp.,* 311 Ill.App.3d 573, 578–79, 243 Ill.Dec. 591, 723 N.E.2d 1192 (2000) (private facts were

clearly alleged); see also *Phillips v. Grendahl,* 312 F.3d 357, 373 (8th Cir.2002); *Andrews v. TRW, Inc.,* 225 F.3d 1063, 1067 (9th Cir.2000), *rev'd on other grounds,* 534 U.S. 19, 122 S.Ct. 441, 151 L.Ed.2d 339 (2001).

Having found no viable causes of action, there is no need for us to address the applicability of the Local Governmental and Governmental Employees Tort Immunity Act. 745 ILCS 10/1–101 *et seq.* (West 2006).

For the foregoing reasons we affirm the trial court's dismissal of plaintiffs' complaints.

Affirmed.

GARCIA, P.J., concurs.

R.E. GORDON, J., dissents.

*****743** ****33** Justice ROBERT E. GORDON, dissenting:
In the case at bar, defendants sent each and every class member a *complete* list of over 1,700 former employees' first and last names, addresses, ***368** marital status, social security numbers, medical and dental insurers, and other health care insurance information. [1] That means, for every class member, over 1,700 people received his or her personal information. In other words, approximately 1,700 people received the personal information of approximately 1,700 other people.

Most of the conclusions in the majority opinion are dependent on its first conclusion. If the first conclusion is removed, then the other dependent conclusions become unpersuasive.

The majority's first conclusion is that the Board's disclosure falls outside of HIPAA's coverage. The majority bases this conclusion entirely on an exclusion in the Code of Federal Regulation. This exclusion states that "employment records *held* by a covered entity in its role as employer" are excluded from HIPAA's protection. (Emphasis added.) 45 C.F.R. § 160.103 (West 2006); see 407 Ill.App.3d at 361–62, 347 Ill.Dec. at 738, 943 N.E.2d at 28.

What the majority misses is that there is a world of difference between "held" and "disclosed." No one objects to the fact that the Board "held" the records. The Board's ability to hold and maintain these records is not at issue here. If the Board had simply held the records—and held on to them-there would be no lawsuit. But the Board did not hold on to them. It is their disclosure, not their holding, that is at issue in this case. [2]

This distinction between holding and maintenance on the one hand, and disclosing on the other, was made clear by the recent amendment to section 1320d–6. Act Feb. 17, 2009, P.L. 111–5, Div. A, Title XIII, Subtitle D, Part 1, § 13409, 123 Stat. 271 (codified as amended at 42 U.S.C. § 1320d-6). Although this amendment was not in effect on the date of the disclosure in question, the amendment merely clarifies the existing statute, rather than adding to it. The amendment clarifies that an individual "shall be considered" to have disclosed individually identifiable health information in violation of this section, if a covered entity both "maintained" the information and then subsequently "disclosed" it. The amendment thus recognizes what we would have assumed even without it, that there is a world of ***369** difference between maintaining or holding on the one hand, and disclosing on the other.

Thus, the exclusion for "held" records, quoted by the majority, does not apply to the case at bar. As a result, the majority's first conclusion, that there is no duty because of this exclusion, is incorrect.

The majority seems to imply that, but for this exclusion, there would be a duty, and we agree. See also *Moss v. Amira,* 356 Ill.App.3d 701, 712, 292 Ill.Dec. 565, 826 N.E.2d 1001 (2005) (Quinn, J., specially concurring) (observing that Illinois law concerning disclosure is generally "far more restrictive" than HIPPA); *****744** ****34** 215 ILCS 5/1021(B) (2006) (providing a private cause of action and damages for the unauthorized disclosure of personal information by "an insurance institution, agent or insurance-support organization").

The majority correctly states:

> "We must first decide whether the Board had a duty to safeguard plaintiffs' personal information under a statutory directive, because where no duty is owed, there is no negligence. *Washington v. City of Chicago,* 188 Ill.2d 235, 239 [242 Ill.Dec. 75, 720 N.E.2d 1030] (1999). Plaintiffs argue that HIPPA (42 U.S.C. § 1320d–6 (West 2006)) [3] provides a statutory basis for the creation of a new duty. A violation of a statute designed to protect human life and property may be used as *prima* facie evidence of

negligence. *Kalata v. Anheuser–Busch Companies, Inc.,* 144 Ill.2d 425, 434–35 [163 Ill.Dec. 502, 581 N.E.2d 656] (1991).[4] HIPPA prohibits the disclosure of 'individually identifiable health information to another person.' 42 U.S.C. § 1320d–6(a)(3) (West 2006)." Op. 407 Ill.App.3d at 361–62, 347 Ill.Dec. at 738, 943 N.E.2d at 28.

This court has already held that the term "individually identifiable health information" in HIPPA includes names, addresses and social security numbers. *Giangiulio v. Ingalls,* 365 Ill.App.3d 823, 839, 302 Ill.Dec. 812, 850 N.E.2d 249 (2006). Specifically, in *Giangiulio,* we found that this term "includes common identifiers such as name, address, birth date, and social security numbers." *Giangiulio,* 365 Ill.App.3d at 839, 302 Ill.Dec. 812, 850 N.E.2d 249. See also *In re: Bextra and Celebrex Marketing*, 2008 WL 5480611, 1, 2008 U.S. Dist. Lexis 111875, 187 (N.D.Cal.2008) ***370** (interpreting the term to include social security numbers).

Our holding in *Giangiulio,* that the term includes names, addresses and social security numbers, is also supported by the definition provided for the term. The term "individually identifiable health information," as used in HIPPA, is defined in both the statute and in the Code of Federal Regulations. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103 (West 2006). This definition includes "demographic information" (1) that is received by an employer; (2) that relates to the provision of or payment for health care; and (3) that identifies an individual. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103 (West 2006). Demographic information is widely understood to include social security numbers, as well as names and addresses. E.g. *In re: Bextra,* 2000 U.S. Dist. Lexis at 187 (discussing "names and addresses, dates of birth, social security numbers * * * and other demographic information"); *Mayfield v. U.S.,* 504 F.Supp.2d 1023, 1027 (D.Or.2007) ("Demographic information included name, date of birth, sex, race, and social security number"). In the case at bar, the names, addresses and social security numbers (1) were received by the employer, (2) related to the provision of or payment for health care, and (3) identified the individual. Thus, our holding in *Giangiulio,* that the *****745** ****35** term includes names, addresses and social security numbers, is also supported by the definition provided for the term.

Since the disclosed names, addresses and social security numbers in the case at bar qualify as "individually identifiable health information," HIPAA applies to the disclosed information. HIPAA also applies to enrollment and disenrollment decisions. 42 U.S.C. § 1320d–2(a)(2)(C) (covered transactions include "[e]nrollment and disenrollment in a health plan"); 45 C.F.R. 160.103.

As the majority already observed, "[a] violation of a statute designed to protect human life and property may be used as *prima facie* evidence of negligence." Op. 407 Ill.App.3d at 361, 347 Ill.Dec. at 738, 943 N.E.2d at 28, citing *Kalata,* 144 Ill.2d at 434–35, 163 Ill.Dec. 502, 581 N.E.2d 656. See also *Noyola v. Board of Education,* 179 Ill.2d 121, 129, 227 Ill.Dec. 744, 688 N.E.2d 81 (1997), discussed recently with approval in *Vancura v. Katris,* 238 Ill.2d 352, 345 Ill.Dec. 485, 939 N.E.2d 328 (Ill.2010). Following the majority's suggestion, I would find that the HIPAA violation serves as *prima facie* evidence of negligence, and I would not dismiss at this early stage of the litigation. *Acosta v. Smith,* 180 N.C.App. 562, 571–72, 638 S.E.2d 246 (N.C.App.Ct.2006) (HIPAA violation used as evidence of "the duty" owed in a negligence case).

In short, the majority and I seem to be in agreement that, but for the exception, there would be a duty. We differ primarily because the majority believes that the exception applies, and I do not.

***371** Most of the remaining conclusions in the majority opinion are based on this first conclusion, and thus are also faulty. For example, later in the opinion, the majority concludes that plaintiff's claim of emotional distress must fail because plaintiffs "failed to establish a duty" on the part of defendants. Op. 407 Ill.App.3d at 363, 347 Ill.Dec. at 739, 943 N.E.2d at 29.[5] However, this conclusion depends on finding, first, that there was no duty under HIPAA. If there was a duty then, at this early stage, plaintiffs would have only to allege, rather than provide evidence, of their anxiety and emotional distress. *Rowe v. Unicare Life and Health Insurance Co.,* 2010 WL 86391, 4–5, 2010 U.S. Dist. Lexis 1576, 11–14 (N.D.Ill., E.D.2010) (although plaintiffs did not allege that the disclosure of their social security numbers and other personal information resulted in unauthorized access by specific persons, plaintiffs' allegations of anxiety were sufficient to withstand a motion to dismiss their emotional distress claim, under Illinois state law).

Similarly, the majority concludes that plaintiffs failed to establish that the Board had a fiduciary duty to avoid disclosure, because the majority finds that plaintiffs cited "no authority supporting such a duty." Op. 407 Ill.App.3d at 363, 347 Ill.Dec. at 739, 943 N.E.2d at 29. Again, this conclusion depends on finding no duty under HIPAA

Since I find that the exclusion, quoted by the majority, does not apply, I must find that the majority's first conclusion is incorrect. Since that first conclusion is the foundation for much of the subsequent opinion, I must respectfully dissent.

I cannot find that HIPAA would allow the disclosure of someone's social security number, marital status, and insurance information, and leave that person without any recourse.

All Citations

407 Ill.App.3d 358, 943 N.E.2d 23, 347 Ill.Dec. 733, 160 Lab.Cas. P 61,101

Footnotes

1 Paragraph 10 of the Cooney second amended complaint alleged that the mailing included "addresses, social security numbers and specific health insurance plan selection information." Paragraph 10 of the Morgan–Wulf third amended complaint alleged that the mailing included "first and last names, addresses, dates of qualification, medical and dental insurers and marital status," as well as social security numbers. The two cases were consolidated.

2 The dictionary defines "hold" as "to have and keep in one's grasp." The American Heritage Dictionary, College Edition 616 (2d ed. 1982).

3 Section 1320d–6(a) provides that "[a] person who knowingly and in violation of this part * * * discloses individually identifiable health information to another person, shall be punished as provided in subsection b" of this section. 42 U.S.C. § 1320d–6(a) (West 2006). Subsection b provides that for a base offense, which is a disclosure committed without false pretenses and without an intent to sell, then the punishment can be up to one year in jail and may include up to a $50,000 fine. 42 U.S.C. § 1320d–6(a) (West 2006).

4 In its brief to this court, defendant Board of Education concedes, as it must, that the violation of a statute designed to protect human life or property may be used as *prima facie* evidence of negligence.

5 The majority does not find that plaintiffs failed to allege emotional distress; rather they simply do not reach this issue. Op. 407 Ill.App.3d at 363, 347 Ill.Dec. at 739, 943 N.E.2d at 29.

KeyCite Yellow Flag - Negative Treatment
Distinguished by Cesare v. Champion Petfoods USA Inc., W.D.Pa., December 20, 2019

196 A.3d 1036
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** De novo review

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

[2] **Appeal and Error** Plenary, free, or independent review

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

[3] **Appeal and Error** Objections and exceptions; demurrer

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.

[4] **Pleading** Hearing and Determination on Demurrer

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

[5] **Appeal and Error** Objections and exceptions; demurrer

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.

[6] **Labor and Employment** Records and confidentiality in general

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.

4 Cases that cite this headnote

[7] **Negligence** Necessity and Existence of Duty

Negligence Duty in general

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.

[8] **Labor and Employment** Records and confidentiality in general

Presence of third-party criminality did not eliminate employer's duty to exercise reasonable care to protect employees against unreasonable risk of harm arising from employer's collection and storage of employees' data on its computer systems.

2 Cases that cite this headnote

[9] **Negligence** Intentional or criminal acts

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.

[10] **Negligence** Economic loss doctrine

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

19 Cases that cite this headnote

[11] **Labor and Employment** Records and confidentiality in general

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.

21 Cases that cite this headnote

***1038** 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. Wettick, R. Stanton, Jr., Judge.

Attorneys and Law Firms

Jamisen A. Etzel, Carlson Lynch Sweet & Kilpela, LLP, Joseph A. Del Sole, Stickman, William Shaw, IV, Del Sole Cavanaugh Stroyd, L.L.C., Gary F. Lynch, Pittsburgh, PA, for Appellant.

John C. Conti, Megan Justine Block, Dickie McCamey & Chilcote PC, Pittsburgh, PA, for Appellee.

James Michael Beck, Reed Smith LLP, Philadelphia, PA, for Amicus Curiae.

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

OPINION

JUSTICE BAER

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 ***1039** 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.

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 ***1040** 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.*

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 ***1041** 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 ***1042** 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." [6] *Id.*

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).

***1043** 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).

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, 642 Pa. 572, 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 ***1044** 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.

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 ***1045** 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)).

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 ***1046** 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 ***1047** (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)).

[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 ***1048** 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]

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 ***1049** 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 page 1051 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*.

UPMC also claims that Employees, focusing upon "misleading dicta" in *Bilt-Rite*, argue for an improperly expansive interpretation of that case which would ***1050** 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]

***1051** 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 ***1052** 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.*

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 ***1053** 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.

This Court granted review to decide "whether [Section] 552 of the Restatement (Second) of Torts [*see supra* at page 1051 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 ***1054** *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.*

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 ***1055** 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, ***1056** 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.

[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.

C. 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 ***1057** 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]

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 1056. [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]

***1058** 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]

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

196 A.3d 1036, 169 Lab.Cas. P 61,919

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 1046, 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 1053 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 1047–48 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 1046–47.

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 1046 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.

929 F.3d 1143
United States Court of Appeals, Ninth Circuit.

UNIVERSAL CABLE PRODUCTIONS, LLC, a Delaware limited liability company; Northern Entertainment Productions, LLC, a Delaware limited liability company, Plaintiffs-Appellants,
v.
ATLANTIC SPECIALTY INSURANCE COMPANY, a New York insurance company, Defendant-Appellee.

No.17-56672
|
Argued and Submitted March 4, 2019 Pasadena, California
|
Filed July 12, 2019

Synopsis

Background: Insureds, which were television production company and its indirect subsidiaries, brought action in diversity against television production insurer, alleging that insurer breached television production insurance policy and covenant of good faith and fair dealing by excluding coverage, under policy's war exclusion, for losses incurred when insured had to move its production out of Israel due to conflict with organization know for violence. The United States District Court for the Central District of California, Percy Anderson, J., 278 F.Supp.3d 1165, granted insurer's motion for summary judgment. Insured appealed.

Holdings: The Court of Appeals, Tashima, Circuit Judge, held that:

[1] contra proferentem did not apply in favor of insured's or insurer's interpretation of contested ambiguous provisions in policy;

[2] customary usage of terms in insurance context applied to war exclusions in policy;

[3] insured carried its burden to show that "war" had special meaning in insurance industry that required hostilities between de jure and de facto governments;

[4] organization known for violence was not de jure or a de facto sovereign, and therefore terrorism by that organization could not be defined as "war" for purposes of interpreting war exclusion;

[5] terrorism by organization known for violence could not be defined as "warlike action by a military force" by "government, sovereign, or other authority"; and

[6] efficient proximate cause of insured production company having to relocate production was firing rockets into Israel where filming was occurring by organization known for violence, and not Israel's retaliatory conduct, and therefore "war" and "warlike actions" exclusions in policy were unenforceable.

Reversed in part, vacated in part, and remanded.

West Headnotes (23)

[1] Federal Courts Summary judgment

Summary judgment orders are reviewed de novo. Fed. R. Civ. P. 56.

1 Cases that cite this headnote

[2] Federal Courts Summary judgment

Federal Courts Summary judgment

When reviewing a summary judgment order, the Court of Appeals must view the evidence in the light most favorable to the nonmoving party and determine whether there are any genuine issues of material fact and whether the district court correctly applied the law. Fed. R. Civ. P. 56.

3 Cases that cite this headnote

[3] Insurance Questions of law or fact

Because the interpretation of an insurance policy is a question of law in California, a court must make its own independent determination of the meaning of the relevant contract language.

[4] Insurance Burden of proof

Under California law, the burden is on the insured to establish that the claim is within the

basic scope of coverage under the insurance policy and on the insurer to establish that the claim is specifically excluded.

[5] **Insurance** Exclusions, exceptions or limitations

Under the contra proferentem doctrine under California law, any ambiguity in an exclusion in an insurance policy is generally construed against the insurer and in favor of the insured.

[6] **Insurance** Ambiguity, Uncertainty or Conflict

Under California law, when the language in an insurance policy is proposed by the insured, the language is not construed against the insurer and may even be interpreted against the insured.

[7] **Insurance** Status or bargaining power of insureds

Under California law, when two sophisticated parties negotiate the terms of an insurance policy, the insured generally cannot invoke the doctrine of contra proferentem.

[8] **Insurance** Status or bargaining power of insureds

Under California law, where the policyholder does not suffer from lack of legal sophistication or a relative lack of bargaining power, and where it is clear that an insurance policy was actually negotiated and jointly drafted, a court need not go so far in protecting the insured from ambiguous or highly technical drafting.

[9] **Insurance** Notice to agents

California courts impute an insurance broker's expertise to its customer-principal.

[10] **Insurance** Status or bargaining power of insureds

Contra proferentem did not apply in favor of insured's or insurer's interpretation of contested ambiguous provisions in television production insurance policy; although provisions consisted entirely of form language, provisions were initially offered by insured's broker and insured was aware of customary meaning of terms in insurance context, and language mirrored insurer's own forms and forms of many insurers.

[11] **Insurance** Usage of trade or business

Insurance War or civil commotion; riot

Customary usage of terms in insurance context applied under California law to war exclusions in television production insurance policy; although insured, as party offering customary usage, was not in insurance trade, it was sophisticated party that frequently engaged in business related to insurance trade and it was represented by broker in insurance trade, and insured showed parties had actual or constructive notice of customary usage. Cal. Civ. Code § 1644; Restatement (Second) of Contracts § 222(3).

[12] **Evidence** Nature of Subject

Insurance Weight and sufficiency

Insured carried its burden under California law to show, under war exclusions in television production insurance policy, that "war" had special meaning in insurance industry that required hostilities between de jure and de facto governments by offering expert testimony that current customary usage of "war" in insurance industry was developed gradually after 9/11 attacks and related litigation to distinguish between acts of war and acts of terror; although expert did not discuss production insurance policy's use of "undeclared war" and its potential implication, insurer did not provide any evidence to contradict expert's conclusion. Cal. Civ. Code § 1644.

[13] **Contracts** Presumptions and burden of proof

Customs and Usages Evidence as to knowledge of custom

Under California law, parties are presumed to contract pursuant to fixed and established usage and custom of the trade or industry.

[14] **Insurance** Plain, ordinary or popular sense of language

Insurance Usage of trade or business

Under California law, plain and ordinary meaning does not apply to the interpretation of an insurance policy if customary usage exists. Cal. Civ. Code § 1644.

[15] **Insurance** War or civil commotion; riot

Organization known for violence was not de jure or de facto sovereign, and therefore terrorism by that organization could not be defined as "war" for purposes of interpreting war exclusion in television production insurance policy under California law; even if that organization exerted control over Gaza, it did not exercise actual control over all of Palestine and agreed, at least in principle, to not disturb Palestinian Authority, which was de jure government of Palestine, and executive branch did not recognize that organization as sovereign, and, instead, designated it as foreign terrorist organization.

1 Cases that cite this headnote

[16] **International Law** Existence and identity of sovereign states

Under international law, a state is an entity that has a defined territory and a permanent population, under the control of its own government, and that engages in, or has the capacity to engage in, formal relations with other such entities. Restatement (Third) of Foreign Relations Law § 201.

[17] **Constitutional Law** Foreign policy and national defense

Who is the sovereign, de jure or de facto, of a territory is not a judicial, but is a political question, the determination of which by the legislative and executive departments of any government conclusively binds the judges.

1 Cases that cite this headnote

[18] **International Law** Existence and identity of sovereign states

A court may examine the status of an area only after the area's sovereignty is politically determined and declared.

[19] **Insurance** War or civil commotion; riot

Organization known for violence was not de jure or de facto sovereign, and therefore terrorism by that organization could not be defined as "warlike action by a military force" by "government, sovereign, or other authority" within meaning of exclusion in television production insurance policy under California law; even if that organization exerted control over Gaza, it did not exercise actual control over all of Palestine and agreed, at least in principle, to not disturb Palestinian Authority, which was de jure government of Palestine, and executive branch did not recognize that organization as sovereign, and, instead, designated it as foreign terrorist organization.

1 Cases that cite this headnote

[20] **Insurance** War or civil commotion; riot

Under California law, term "warlike action" has a special meaning in the insurance industry that derives from the typical exclusion for "warlike operations" which requires (1) operations of such a general kind or character as belligerents have recourse to in war, and (2) that such operations be carried out by the military forces of a sovereign or quasi-sovereign government.

[21] **Insurance** War or civil commotion; riot

Insurance Proximate Cause

Efficient proximate cause of insured production company having to relocate production was firing of rockets into Israel where filming was occurring by organization known for violence, and not Israel's retaliatory conduct, and therefore "war" and "warlike actions" exclusions in television production insurance policy were unenforceable under California law against claim for coverage of relocation costs.

[22] **Insurance** Exclusions and limitations in general

Insurance Proximate Cause

Insurance policy exclusions are unenforceable to the extent that they conflict with the California Insurance Code and the efficient proximate cause doctrine.

[23] **Insurance** Exclusions and limitations in general

Insurance Proximate Cause

Under California law, an excluded risk contributing to a loss does not preclude coverage if such a risk was a remote cause of the loss.

Attorneys and Law Firms

***1146** Amanda Kate Bonn (argued) and Kalpana Srinivasan, Susman Godfrey LLP, Los Angeles, California; Jacob W. Buchdahl, Susman Godfrey LLP, New York, New York; for Plaintiffs-Appellants.

Margaret A. Grignon (argued) and Anne M. Grignon, Grignon Law Firm LLP, Long Beach, California; Michael Keeley and Carla. C. Crapster, Strasburger & Price LLP, Dallas, Texas; for Defendant-Appellee.

Appeal from the United States District Court for the Central District of California, Percy Anderson, District Judge, Presiding, D.C. No. 2:16 cv-04435 PA

Before: Ransey Guy Cole, Jr.,* A. Wallace Tashima, and Jacqueline H. Nguyen, Circuit Judges.

OPINION

TASHIMA, Circuit Judge:

In late June and through July of 2014, Hamas fired rockets from Gaza into Israel. Because of these hostilities, the plaintiffs, Universal Cable Productions, LLC, and Northern Entertainment Productions, LLC (collectively "Universal"), moved the production of their television series *Dig* out of Jerusalem. Universal incurred significant ***1147** expenses during this move and filed an insurance claim for coverage of those costs under a television production insurance policy (the "Policy").

Universal's insurer, defendant Atlantic Specialty Insurance Company ("Atlantic"), denied coverage, stating that although the Policy covered expenses related to terrorism, the hostilities were excluded from coverage. Atlantic relied on the Policy's war exclusions, which excluded coverage for expenses resulting from "war," "warlike action by a military force," or "insurrection, rebellion, [or] revolution." Atlantic concluded that Hamas' actions were excluded acts of war.

Universal responded that these war exclusions did not apply because the terms had a specialized meaning in the insurance context. Specifically, "war" and "warlike action by a military force" required hostilities between de jure or de facto sovereigns. Universal argued that Hamas was not acting as a sovereign, and thus its actions were not excluded from coverage.

The district court granted summary judgment to Atlantic and held that, instead of the specialized meanings of "war" and "warlike action," the relevant definitions were the ordinary and plain meanings of each term. The district court held that under its interpretation, Hamas' actions clearly constituted "war" and "warlike action by a military force," rather than acts of terrorism. Based on its interpretation of those two exclusions, the district court also granted summary judgment to Atlantic on Universal's bad faith claim. [1]

Although this case concerns the Israeli-Palestinian conflict and hostilities between different factions in the region, the legal analysis boils down to simple contractual interpretation. Section 1644 of the California Civil Code requires us to apply the specialized meaning of a term – instead of the plain, ordinary meaning – when that specialized meaning has

been developed from customary usage in a given industry and when both parties have constructive notice of that usage. Both "war" and "warlike action by a military force" have a specialized meaning in the insurance context and the parties had, at the least, constructive notice of the meaning. The district court erred when it failed to apply that meaning. Under that specialized meaning, both "war" and "warlike action by a military force" require hostilities between either de jure or de facto sovereigns, and Hamas constitutes neither.

Accordingly, we reverse the district court's entry of summary judgment in favor of Atlantic on the first two war exclusions and hold that Atlantic breached its contract when it denied coverage by defining Hamas' conduct as "war" or "warlike action by a military force." Because the district court did not address the third war exclusion – whether Hamas' actions constituted "insurrection, rebellion, or revolution" – we remand for the district court to address that question in the first instance. The district court's grant of Atlantic's motion for summary judgment on Universal's bad faith claim turned on its erroneous analysis of the first two war exclusions; accordingly, we vacate the grant of summary judgment on Universal's bad faith claim and remand for proceedings consistent with this opinion.

I. Background

A. Historical Background

We begin with the history between Israel, Palestine, and Hamas.[2] The Palestinian ***1148** political identity emerged between 1923 and 1948. Jim Zanotti, *Cong. Research Serv.*, RL34074, *The Palestinians: Background and U.S. Relations* 2 (2015) ("2015 CRS Palestine Report"). In 1947, the United Nations intended to create two states in what are now Israel and Palestine – one Jewish and one Arab – but for reasons that are still disputed, the U.N. ultimately founded only the Jewish state of Israel. *Id.* In June 1967, Israel gained control over the entire area that had historically constituted Palestine. *Id.* at 3. Ultimately, Israel annexed only East Jerusalem and the Golan Heights, leaving the West Bank and Gaza under Israeli occupation, but not under Israeli governance. *Id.*

In the mid-1990s, the Palestinian Authority was granted limited rule in Gaza and parts of the West Bank. *Id.* at 4, 26. In 2005, Israel unilaterally withdrew from Gaza, leaving control to the Palestinian Authority. *Id.* at 47. According to a U.S. Congressional Research Service report, "[a]lthough not a state, the [Palestinian Authority] is organized like one – complete with democratic mechanisms; security forces; and executive, legislative, and judicial organs of governance." *Id.* at 26. The legislative branch is called the Palestinian Legislative Council. *Id.* Fatah and Hamas are the largest Palestinian political movements. *Id.* at 48.

Hamas was founded in 1987. Jim Zanotti, *Cong. Research Serv.*, R41514, *Hamas: Background and Issues for Congress* 400 (2010) ("2010 CRS Hamas Report"). Hamas is committed "to the destruction of Israel and the establishment of an Islamic State in all of historic Palestine, comprised of present-day Israel, the West Bank, and Gaza." 2015 CRS Palestine Report at 33. Hamas' command center is in Gaza. *Id.* In 2006, Hamas won a majority of the seats in the Palestinian Legislative Council. *Id.* at 26. Since then, Hamas has provided social services in the Gaza Strip, collected revenue, established a judicial branch of sorts, and received some assistance from foreign governments. According to the Congressional Research Service, there has been tension between Hamas' activities as a "militant organization uncompromisingly opposed to Israel in defiance of international opprobrium" and Hamas' activities as a "de facto government in Gaza." 2010 CRS Hamas Report at 17. Hamas itself has drawn "a bright line bifurcating the organization's leadership from its members in the Gaza government." *Id.* at 18. Furthermore, the same Report notes that any reference "to the government in Gaza as the 'Hamas regime' does not mean that all or even most of the people employed in ministries, civil service positions, and even security forces are necessarily members of Hamas or even Hamas sympathizers." *Id.* at 19.

In June 2014, Hamas reached an agreement with Fatah to establish a consensus Palestinian Authority government. 2015 CRS Palestine Report at 1. As part of the agreement, Hamas agreed to give up any formal responsibility for governing Palestine, and Hamas' members no longer served as government ministers. *Id.* at 1, 29. Nevertheless, Hamas' security forces remained in Gaza and have continued to exercise some control there. *Id*. at 29.

The United States has never recognized Palestine or Gaza as sovereign territorial nations, nor has it ever recognized Hamas as a sovereign or quasi-sovereign (i.e., a de jure or de facto government). In fact, since 1997, the United States has designated Hamas as a Foreign Terrorist Organization under the Immigration and Nationality Act, 8 U.S.C. § 1189(a)(1). Since 2007, Hamas has had a history of firing rockets into Israel. The United States has continued to designate Hamas

as a Foreign Terrorist Organization and does not negotiate or enter into treaties with Hamas.

***1149** *B. Factual Background*

For the period from January 1, 2014, to June 30, 2015, Atlantic issued a television production insurance policy to Universal. The Policy covered losses that are "a direct result of an unexpected, sudden or accidental occurrence entirely beyond your control to include ... [i]mminent peril, defined as certain, immediate and impending danger of such probability and severity to persons or property that it would be unreasonable or unconscionable to ignore." The Policy, which was negotiated before December 2013, covered loss caused by terrorism if that loss was not otherwise excluded.

The relevant exclusions for our analysis are the four war exclusions:

1. *War*, including undeclared or civil war; or

2. *Warlike action* by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign, or other authority using military personnel or other agents; or

3. *Insurrection, rebellion, revolution*, usurped power, or action taken by the governmental authority in hindering or defending against any of these. Such loss or damage is excluded regardless of any other cause or event contributed concurrently or in any sequence to the loss.

4. Any weapon of war including atomic fission or radioactive force, whether in time of peace or war ....

Universal's broker, Aon/Albert G. Ruben Insurance Services, Inc., initially sent the first three exclusions above to Atlantic. The language was standard insurance industry form language from the Insurance Service Office, Inc.'s ("ISO") standard Form No. CA00200310. Atlantic subsequently edited some of the policy language and added the fourth war exclusion.

On December 3, 2013, Universal's broker emailed Atlantic about three developments: (1) noting "that there is a production in development that is tentatively starting up in February 2014 and filming in Israel," specifically in "Tel Aviv and Jerusalem"; (2) stating "[w]e wanted to get some feedback from you on what issues we may have covering the production under the blanket policy – any additional premiums or exclusions beyond our standard terms"; and (3) asking Atlantic to let Universal "know what [Atlantic's] concerns may be on this."

The broker then had a discussion with Atlantic "regarding issues they may have with the project entitled 'Dig,' potentially working in Israel." During that conversation, Atlantic indicated it "understands that [Universal] takes seriously safety and security precautions on every production but that they were particularly concerned about those precautions in this locale." As a result, Atlantic asked Universal to provide "specific information regarding the security efforts that will be taken during the course of principal photography." Atlantic then concluded that it would "not be imposing any additional premium or additional coverage terms on *Dig* relating to the work in Israel," the "primary reason for [which] is [its] confidence in the safety and security measures that will be taken during the production." Atlantic did not change the policy's terms, add any exclusions – such as a terrorism exclusion – or charge any additional premium.

1. June 2014 Conflict

After *Dig* began production in Israel, three Israeli teenagers were kidnapped on June 12, 2014, and Hamas was suspected of involvement in the kidnappings. On June 30, 2014, the bodies of the three missing teenagers were recovered, and there were signs indicating Hamas was ***1150** involved. On July 2, 2014, a Palestinian teenager was abducted and killed by Israelis, presumably in retaliation for the kidnapping of the Israeli teens. In late June or early July 2014, Hamas began firing rockets from Gaza into Israeli civilian populations, significantly increasing the number of attacks around July 8. [3] Israel responded by launching a campaign against Hamas, called "Operation Protective Edge."

On July 8, the U.S. State Department issued a warning regarding the "safety and security of civilians" in Israel, specifically in Jerusalem. *Dig* filming was scheduled to take place in Jerusalem over the next few weeks. Two days later, the Universal security team advised the *Dig* production team that the "security environment in Israel currently prohibits NBCU Security from being able to guarantee the safety and security of our employees, production partners and associated crew and talent." The security team indicated that "current rocket attacks" appeared "to target locations to be used in forthcoming filming" and it was concerned about "acts of terrorism within Israel."

2. Denial of Claim Coverage

On July 11, 2014, the day after receiving the security team's advice, Universal decided to postpone production for a week and informed Atlantic. Four days later, Universal's broker notified Atlantic in writing of Universal's claim relating to the one-week delay of *Dig*. Atlantic's Chief Underwriting Officer, Peter Williams, then wrote in an internal email to the claims investigator stating that the claim was a "covered claim they have immanent [sic] peril. Unless you are going to invoke the war exclusion." Atlantic's senior claims investigator responded to Williams:

> Any chance you happen [sic] to suggest that they push for more than just the week, since the crew needs to be advised at least one week in advance for a push and since a ground war still might occur.

The next day, Atlantic's Assistant Vice President stated internally that "it looks like we need to have a lot further discussion about this." Atlantic had never applied the war exclusions before this claim.

Due to escalating violence, Universal decided to move the *Dig* production out of Israel altogether and notified Atlantic of that decision on July 17, 2014 That same day – two days after Universal's broker submitted the initial written claim – Atlantic denied coverage under the war exclusions. Atlantic's supervising claims examiner could not recall any other claim where a coverage determination was made in two days, stating that this denial occurred on an expedited timeframe. During the two days between the filing of the claim and Atlantic's denial of coverage, Atlantic employees engaged in the following analysis: They conducted Google searches for news articles about Hamas and Israel and reviewed one case, in which the court declined to apply war exclusions to the act of Palestinian and Lebanese sub-national groups bombing a hotel in Beirut. *See Holiday Inns Inc. v. Aetna Ins. Co.*, 571 F. Supp. 1460, 1503 (S.D.N.Y. 1983). Atlantic did not consult the policy's underwriter about the intent regarding the exclusions, although its usual practice was to engage in such a consultation.

Two weeks after denying coverage, Atlantic sent Universal a denial letter. Atlantic's letter stated that "[r]ockets launched toward areas where filming is taking place would no doubt reasonably constitute" a covered imminent peril. Atlantic also stated, ***1151** however, that "[t]he question now is not whether the loss falls within the insuring clause but whether the war exclusion" applies. Atlantic concluded that "the extra expense associated with the move is not covered under [the Policy] because of the exclusion for war and warlike action" – the first and second war exclusions.

C. Procedural History

Universal filed suit against Atlantic, asserting claims for breach of contract and breach of the implied covenant of good faith and fair dealing. During litigation, Atlantic took the position that all four contractual war exclusions barred coverage.

Following discovery, Atlantic moved for summary judgment on both claims. Universal filed a cross-motion for partial summary judgment on its first claim: Atlantic breached the contract. In June 2017, the district court granted Atlantic's motion in a short minute order without further explanation. Four months later, the district court issued a written order granting Atlantic's motion and denying Universal's motion, holding that the first two war exclusions barred coverage and that Atlantic did not act in bad faith. With regard to the war exclusions, the district court concluded that under California law, the exclusions should be understood in their popular and ordinary sense and that "[s]uch a conflict easily would be considered a 'war' by a layperson." The district court rejected Universal's argument that "war" has a special meaning through usage in the insurance industry. The district court did not address the third and fourth exclusions.

II. Standard of Review

[1] **[2]** Summary judgment orders are reviewed de novo. *Lopez-Valenzuela v. Arpaio*, 770 F.3d 772, 777 (9th Cir. 2014) (en banc). We must view [ ] "the evidence in the light most favorable to the nonmoving party" and "determine 'whether there are any genuine issues of material fact and whether the district court correctly applied the law.' " *Pension Tr. Fund for Operating Eng'rs v. Fed. Ins. Co.*, 307 F.3d 944, 949 (9th Cir. 2002) (internal quotation marks and citation omitted).

[3] **[4]** "Because the interpretation of an insurance policy is a question of law, this Court must make its own independent determination of the meaning of the relevant contract

language." *Conestoga Servs. Corp. v. Exec. Risk Indem.*, 312 F.3d 976, 981 (9th Cir. 2002). "The burden is on the insured to establish that the claim is within the basic scope of coverage and on the insurer to establish that the claim is specifically excluded." *MacKinnon v. Truck Ins. Exch.*, 31 Cal.4th 635, 3 Cal.Rptr.3d 228, 73 P.3d 1205, 1213 (2003).

The parties do not dispute that the claimed loss is a covered "imminent peril." Thus, Atlantic bears the burden of demonstrating that the war exclusions require denial of coverage. *See id.*

III. Contra Proferentem Does Not Apply

[5] **[6]** **[7]** **[8]** **[9]** With regard to interpreting the Policy's language, both parties argue that any ambiguity should be construed in their favor. Under the doctrine of contra proferentem, any ambiguity in an exclusion is generally construed against the insurer and in favor of the insured. *Fireman's Funds Ins. Co. v. Fibreboard Corp.*, 182 Cal.App.3d 462, 227 Cal. Rptr. 203, 206 (1986). When the language in a policy is proposed by the insured, however, the language is not construed against the insurer and may even be interpreted against the insured. *Id.* at 207. Furthermore, when two sophisticated parties negotiate the terms of the policy, the insured generally cannot invoke the doctrine of contra proferentem. ***1152** *Garcia v. Truck Ins. Exch.*, 36 Cal.3d 426, 204 Cal.Rptr. 435, 682 P.2d 1100, 1106 (1984). "[W]here the policyholder does not suffer from lack of legal sophistication or a relative lack of bargaining power, and where it is clear that an insurance policy was actually negotiated and jointly drafted, we need not go so far in protecting the insured from ambiguous or highly technical drafting." *AIU Ins. Co. v. Superior Court*, 51 Cal.3d 807, 274 Cal.Rptr. 820, 799 P.2d 1253, 1265 (1990). [4]

The district court, citing *AIU*, held that there was no presumption in favor of Universal here because (1) Universal's broker provided the contested language to Atlantic, and (2) Universal is a sophisticated party with bargaining power. In *AIU*, the insured "unquestionably possesse[d] both legal sophistication and substantial bargaining power." *Id.* The question was whether the disputed policy term had a technical meaning (as the insurer contended) or had a plain and ordinary meaning (as the insured contended). *Id.* The record lacked any evidence that the provision in question had been negotiated or jointly drafted. *Id.* Because there was no evidence the parties intended to adopt a technical meaning, which would have excluded coverage for the insured, the Supreme Court of California held that the ambiguity would be resolved against the party responsible for the inclusion of the provision: the insurer. *Id.*

[10] Universal argues that, similarly, any ambiguity here should be construed against the insurer. Atlantic responds that, unlike *AIU*, Universal's broker provided the policy language in question, and any ambiguity should instead be construed against the party that offered the language: Universal.

Universal counters that "a distinction must be made between a broker requesting certain language cut-and-pasted from other policies issued by an insurer and a broker drafting or editing specific policy language." 8 Bus. & Comm. Litig. Fed. Cts. § 90:42 (4th ed. 2017). "The mere inclusion of standard form language from another policy at the request of a policyholder or its broker should not result in a departure from the rule of contra proferentem." *Id.* Here, the disputed language was insurance industry form language from the ISO's standard Form No. CA00200310. "Policy forms developed by ISO are approved by its constituent insurance carriers and then submitted to state agencies for review," and "[m]ost carriers use the basic ISO forms, at least as the starting point for their general liability policies." *Pardee Const. Co. v. Ins. Co. of the West*, 77 Cal.App.4th 1340, 92 Cal. Rptr. 2d 443, 456 n.15 (2000).

Contra proferentem stems "from the fact that the insurer typically drafts policy language, leaving the insured little or no meaningful opportunity or ability to bargain for modifications." *AIU*, 274 Cal.Rptr. 820, 799 P.2d at 1265. Although *AIU* acknowledged that the insured there "unquestionably possesse[d] both legal sophistication and substantial bargaining power," it opted to apply contra proferentem anyway because the parties had not negotiated a technical meaning. *Id.* The California Supreme Court concluded that it would still construe the terms against the insurer because "such provisions, drafted by the insurers, are highly uniform in content and wording" and there was "no evidence ... suggesting that the provisions in question were actually negotiated or jointly drafted." *Id.* Moreover, the court was concerned about the insurer interpreting terms in a technical manner, thus denying ***1153** coverage when the insured was not on notice about the technical meaning.

AIU is distinguishable from the case before us. Here, the provisions were initially offered by Universal's broker (although they consisted entirely of form language). Moreover, Universal does not rebut the district court's conclusion that it is a sophisticated party. Most importantly, Universal – the insured – is asking the court to interpret policy language under the customary meaning in the insurance context. Unlike *AIU*, where the court was concerned about restrictive, technical language being construed against the insured without notice, Universal is aware of the customary meaning in the insurance context and asks us to apply that meaning instead of the plain and ordinary meaning. The typical concerns animating contra proferentem do not exist here.

Accordingly, we decline to apply contra proferentem in favor of Universal's interpretation. We also decline to apply contra proferentem in favor of Atlantic. The language here mirrors Atlantic's own forms – and the forms of many insurers – and does not warrant a presumption in favor of Atlantic's interpretation either. The parties provide no reason to protect the insured or the insurer from any ambiguous drafting in this instance. [5]

IV. Section 1644 and Customary Usage

[11] The district court erred in holding that Atlantic met its burden of demonstrating that the first two war exclusions apply. To the contrary, the record demonstrates that neither exclusion applies here. Atlantic breached its contract by denying Universal coverage on that basis.

Under California law, the terms in an insurance policy are "understood in their ordinary and popular sense, rather than according to their strict legal meaning; unless used by the parties in a technical sense, or *unless a special meaning is given to them by usage, in which case the latter must be followed*." Cal. Civ. Code § 1644 (emphasis added). A district court's failure to consider the special meaning of a term in "industry custom and practice" is reversible error. *See Nat'l Am. Ins. Co. of Cal. v. Certain Underwriters at Lloyd's London*, 93 F.3d 529, 537 (9th Cir. 1996). Here, the district court erred in holding that the war exclusions should be understood in their ordinary and plain sense, instead of applying the special meaning of the terms in the insurance context.

We note that § 1644 's requirement that courts apply customary usage is cabined by a few requirements. Generally, a party asking a court to apply customary usage would be engaged in the relevant trade – here, the insurance trade. *See* Restatement (Second) of Contracts § 222(3) (stating that "[u]nless otherwise agreed, a usage of trade in the *vocation or trade in which the parties are engaged or a usage of trade of which they know or have reason to know* gives meaning to or supplements or qualifies their agreement" (emphasis added)). Although Universal is not in the insurance trade, it is a sophisticated party that frequently engages in business related to the insurance trade. Moreover, it is represented by a broker – who is Universal's agent – in the insurance trade.

***1154** If any party is not engaged in the trade, the party offering customary usage must show the parties had actual or constructive notice of the customary usage. [6] *See id.* § 220(1) (stating that "[a]n agreement is interpreted in accordance with a relevant usage if each party knew or had reason to know of the usage and neither party knew or had reason to know that the meaning attached by the other was inconsistent with the usage"). Here, Universal has met that burden. As discussed below, Universal provides unrebutted expert evidence demonstrating the customary usage of "war" and "warlike action by a military force" in the insurance context. Caselaw and insurance treatises buttress Universal's argument that ordinary, popular meanings of these terms do not control in this context. Moreover, as Universal notes, Atlantic's own denial letter stated that "Appleman on Insurance discusses exclusions for war, including the meaning of war and similar terms. 'War is a "course of hostility" between "states or state-like entities." ' " And Universal's expert noted that "if the policy does not contain a terrorism exclusion, there is a reasonable expectation that acts of terrorism by a known terrorist organization, regardless of however else they may be characterized, will be covered." Universal stated that it reasonably expected the exclusionary clause would be interpreted according to customary usage, especially after the December 2013 emails about the policy's coverage in Israel. At the least, both parties should have known the customary usage of "war" and "warlike action" in the insurance context.

Accordingly, we apply the customary usage of the terms in the insurance context here.

A. The First War Exclusion

1. *The special meaning of "war" in the insurance context*

[12] Universal provided the district court with substantial unrebutted evidence that, in the insurance context, the term "war" has a special meaning that requires the existence of hostilities between de jure or de facto governments. Universal relied on caselaw, insurance treatises, and expert testimony to show the existence of this industry custom.

With regard to caselaw, Universal relied on a set of cases defining "war" in accordance with the international law definition: war refers to and includes *only* hostilities carried on by entities that constitute governments at least de facto in character. *See Pan Am. World Airways v. Aetna Cas. & Surety Co.*, 505 F.2d 989, 1012 (2d Cir. 1974); *see also Holiday Inns*, 571 F. Supp. at 1503 (holding in the insurance context that "war" must be "between sovereign or quasi-sovereign states"). The courts in both *Pan Am* and *Holiday Inns* refused to treat violent actions by Palestinian terrorist organizations targeting civilians as falling within the "war" exclusion. *Pan Am*, 505 F.2d at 1016 (declining to find that hijacking carried out by the Popular Front for the Liberation of Palestine fell within war exclusions); *Holiday Inns*, 571 F. Supp. at 1472, 1503 (declining to find that mortar shelling by Palestinian and Lebanese factions in Beirut fell within war exclusions). *Holiday Inns* specifically rejected the argument that a "common meaning" of war applies in the insurance context, holding instead that "[i]n commercial litigation arising out of insurance policies, words and phrases are construed 'for insurance purposes' – a context quite different from those of politics or journalism." ***1155** 571 F. Supp. at 1464 (quoting *Pan Am*, 505 F.2d at 993). The Second Circuit in *Pan Am* concluded that "war is a course of hostility engaged in by entities that have at least significant attributes of sovereignty." *Pan Am*, 505 F.2d at 1012.

Similarly, a leading insurance treatise recognizes that in this context, " 'war' is defined as the employment of force between governments or entities essentially like governments, at least de facto," because "[w]ar is often viewed as the method by which a nation prosecutes its right by force." 10A Couch on Insurance § 152:3 (3d ed. 2017). [7] Another treatise notes that "while the sovereign act and war exclusions are not entirely irrelevant to coverage of terrorist related losses, an insurer seeking to invoke these exclusions faces steep factual, legal and political hurdles" because of caselaw defining war as the act of a sovereign. 32-191 Appleman on Insurance Law & Practice Archive § 191.02 (2d ed. 2011).

With regard to the record, Universal's insurance industry expert stated that under insurance industry custom, "an underwriter cannot merge the two concepts and say that 'an act of terrorism' can be also an 'act of war,' " because "if the policy does not contain a terrorism exclusion, there is a reasonable expectation that acts of terrorism by a known terrorist organization, regardless of however else they may be characterized, will be covered." Atlantic did not rebut this argument; nevertheless, the district court did not consider Universal's expert testimony regarding the special meaning of "war" in the insurance context. Moreover, Universal explained to the district court that even Atlantic's denial letters noted that "[w]ar is a course of hostility between states or state-like entities," and "[t]o constitute a de facto state, a group must have significant attributes of sovereignty." The district court did not address this fact either.

[13] The district court held that Universal "[did] not present specific evidence from the negotiation or drafting of the Policy reflecting the parties' intention to use any technical or special meaning of 'war,' " or any specific evidence that "the parties or [Universal's broker] had in mind the more restrictive meaning of 'war' discussed in *Pan Am* or *Holiday Inns* when the Policy was negotiated." (citing Cal. Civ. Code § 1644). In coming to this conclusion, the district court conflated the various provisions of § 1644 and shifted the burden to Universal without any explanation. Section 1644 states that words in a contract are "understood in their ordinary and popular sense ... unless used by the parties in a technical sense, or *unless* a special meaning is *given to them by usage*, in which case the latter *must* be followed." Cal. Civ. Code § 1644 (emphases added). The former provision requires that the terms have been "used by the parties in a technical sense," but the latter requires simply that the special meaning of the terms be "given to them by usage." *Id*. This interpretation is supported by California law, which provides that "[p]arties are presumed to contract pursuant to fixed and established usage and custom of the trade or industry." *S. Pac. Transp. Co. v. Santa Fe Pac. Pipelines, Inc.*, 74 Cal.App.4th 1232, 88 Cal. Rptr. 2d 777, 785 (1999); *see also Nat'l Am. Ins. Co. of Cal.*, 93 F.3d at 537 (holding that "[o]rdinary rules of construction permit custom or usage ***1156** evidence both to explain the meaning of language and to imply terms, where no contrary intent appears from the terms of the contract").

Contrary to the district court's holding, California law does not require Universal to introduce "specific evidence from the negotiation or drafting of the Policy reflecting the parties' intention" to use any "special meaning of 'war.' " Such an

interpretation would conflate § 1644 's distinction between technical meaning and customary usage. Instead, as noted above in this Part IV, the only requirement is that the parties had at least constructive notice of the usage, which they did here. Atlantic failed to show that "war" did not have a special meaning in the insurance context, especially considering Universal's ample evidence to the contrary.

Atlantic does not explicitly dispute that "war" has a special meaning in the insurance industry requiring hostilities between de jure and de facto governments. Atlantic instead focuses on whether California law requires this special meaning.

[14] First, Atlantic argues that under *Sony Computer Entertainment America, Inc. v. American Home Assurance Co.*, 532 F.3d 1007, 1013 (9th Cir. 2008), Universal bears the burden to submit some extrinsic evidence of the parties' intent to adopt a special meaning. *Sony* addressed technical meaning, which – unlike customary usage – does require a showing of intent. Furthermore, § 1644 provides no qualifications or requirement of intent to its mandate regarding the application of customary usage. As discussed, Atlantic's interpretation would render § 1644 's distinction between technical meaning and customary usage surplusage. Moreover, Atlantic's reliance on interpretive rules requiring plain meaning in other contexts is misplaced, given § 1644 's specific requirement that plain and ordinary meaning does not apply if customary usage exists. *See Burger v. Emp. Ret. Sys.*, 101 Cal.App.2d 700, 226 P.2d 38, 39–40 (1954) (requiring plain and ordinary meaning for constitutional measures adopted by popular vote); *Kaiser v. Hopkins*, 6 Cal.2d 537, 58 P.2d 1278, 1279 (1936) (requiring plain and ordinary meaning for constitutional measures because they are adopted "by the meaning apparent on its face"); *Vandegrift v. Bd. of Supervisors*, 23 Cal.App.3d 228, 100 Cal. Rptr. 87, 90–91 (1972) (same).

Second, Atlantic argues that the parties did not choose to use "war" in any formal or technical sense because of the inclusion of "undeclared war" in the first exclusion. Atlantic relies on two non-binding cases that addressed whether insurance policies applied to undeclared wars during World War II. *See N.Y. Life Ins. Co. v. Durham*, 166 F.2d 874, 876 (10th Cir. 1948) (holding that where an insurance policy expressly excluded losses due to "undeclared war," the parties expressly "chose not to use the word 'war' in its technical or formal sense"); *Gagliormella v. Met. Life Ins. Co.*, 122 F. Supp. 246, 249 (D. Mass. 1954) (holding that a policy excluded undeclared war between "United States and another country"). These cases are distinguishable for three reasons. First, both cases discuss war between de jure governments, which the Israeli-Hamas conflict was not. *See* Part IV.A.2. Second, the Tenth Circuit's interpretation of "undeclared war" as an express indication of the parties' intent to avoid the special meaning of the term "war" does not apply under California law, which mandates the application of a special meaning under § 1644. Third, Universal's unrebutted expert testimony notes that the current customary usage of "war" in the insurance industry was developed gradually after the 9/11 attacks (and related litigation) to distinguish between acts of war and acts of terror in the insurance context. Although Universal's expert does not discuss the contract's use of "undeclared war" ***1157** and its potential implication here, Atlantic has not provided any evidence to contradict the expert's conclusion that "war" has a specialized meaning in this instance.

Finally, Atlantic relies on three cases – all outside the insurance context – holding that the 9/11 terrorist attacks were acts of war. Atlantic failed to recognize, however, that the district court in *In re September 11 Litigation*, 931 F. Supp. 2d 496, 514 (S.D.N.Y. 2013), *aff'd*, 751 F.3d 86, 90–91 (2d Cir. 2014), cautioned that its holding in the CERCLA [8] context should be "read narrowly, fitting the facts of this case only" and "should not be a precedent for cognate laws of insurance." The Second Circuit reaffirmed this distinction, noting that courts should still have a "narrow reading of a contractual 'act of war' exclusion," but the "remedial purpose of CERCLA is both different and unrelated" to typical contractual terms. *In re Sept. 11 Litig.*, 751 F.3d at 92–93. Similarly, Atlantic's reliance on *Hamdan v. Rumsfeld*, 548 U.S. 557, 126 S.Ct. 2749, 165 L.Ed.2d 723 (2006), and *Hamdi v. Rumsfeld*, 542 U.S. 507, 124 S.Ct. 2633, 159 L.Ed.2d 578 (2004), both habeas cases, fails to recognize that "war" has a special meaning in the insurance context.

Outside of these inapposite cases, Atlantic does not dispute that the insurance industry has a customary usage that limits exclusions for "war" to hostilities between de jure or de facto sovereigns. The district court erred by failing to apply this special meaning. Because the district court should have applied the special meaning, we need not address whether the district court's analysis of the plain and ordinary meaning of "war" was incorrect.

2. *Hamas is neither a de jure nor a de facto sovereign*

[15] The district court erroneously concluded that Universal did not meet its burden to demonstrate that "Hamas is a terrorist group for all purposes," and that the war exclusion applied. But Universal does not need to show that Hamas acts as a terrorist group "for all purposes" in order to prove that the policy covers Hamas' conduct. Instead, the appropriate question is whether Hamas was acting as a de jure or de facto sovereign at the time of the 2014 hostilities.

[16] "Under international law, a state is an entity that has a defined territory and a permanent population, under the control of its own government, and that engages in, or has the capacity to engage in, formal relations with other such entities." Restatement (Third) of Foreign Relations Law § 201 (1987); *see also Holiday Inns*, 571 F. Supp. at 1499–1500. The United States, the European Union, Canada, Australia, and multiple other countries do not recognize Hamas as a legitimate authority in either Palestine or Gaza – the relevant territories for our analysis. Hamas does not engage in formal relations on behalf of Palestine (or even Gaza). The record does not indicate that Hamas controls Palestine's borders, airspace, or immigration. This is particularly important when we consider Hamas' recognition of the Palestinian Authority's control over all governing functions.

Atlantic argues that Hamas has significant attributes of sovereignty, which supports the district court's conclusion that Hamas is a de facto sovereign. Atlantic relies on *Pan Am* and *Holiday Inns* in coming to this conclusion, but Atlantic cherry-picks selected portions of those ***1158** cases' descriptions of what constitutes a de facto sovereign.

Pan Am focused on whether the entity in question had "significant attributes of sovereignty," or whether it was an entity "that constitute[d] government[ ] at least de facto in character," similar to "enemy nations at war with one another." 505 F.2d at 1012. Atlantic incorrectly states that *Pan Am* described a de facto government as "a force [controlling] a substantial territory with trappings of state." *Id.* at 1009. That definition was not *Pan Am*'s holding, but rather part of a summary of the parties' arguments before the district court. To the contrary, *Pan Am* held that a terrorist group was not a de facto government because it was not acting on behalf of the recognized government. *Id.* at 1012.

Atlantic also argues that in *Holiday Inns*, the court held war can exist between de facto governments, meaning entities that "stake out and maintain adverse claims to territory." 571 F. Supp. at 1500. Atlantic does not include the full quotation:

> *It is not sufficient to achieve such status that the group or entity in question occupy territory* within the boundary of the sovereign state upon the consent of that state's de jure government. That is so, even if that government's consent extends to permitting its guests to exercise considerable control and autonomy within the camps or other facilities in which they dwell. "De facto governments" manifest "attributes of sovereignty" when they stake out and maintain adverse claims to territory, *accompanying those claims with declarations of independence and sovereignty*.

Id. (emphases added). *Holiday Inns* also held that private militias do not constitute de facto sovereigns when a de jure government exists in the form of executive and legislative leadership (even if that de jure government functions with "considerable difficulty"). *Id.* *Holiday Inns* specifically noted that a de facto sovereign would not recognize the de jure government's sovereignty, let alone agree not to disturb it. *Id.* Here, the Palestinian Authority is the de jure government, and Hamas has recognized the Palestinian Authority as the controlling government of Palestine. *Holiday Inns* therefore supports the conclusion that Hamas is not the de facto sovereign of Palestine.

Atlantic argues that "Hamas operates political, military, and social branches," and its social service branch operates hospitals, schools, and other services, just like any other government. *See United States v. El-Mezain*, 664 F.3d 467, 485–86 (5th Cir. 2011); *see also Estates of Ungar v. Palestinian Auth.*, 304 F. Supp. 2d 232, 250 (D.R.I. 2004) (concluding that "Hamas operates through a political branch and a military branch"). Atlantic does not dispute that Gaza is part of Palestine and not its own sovereign state. At most, Hamas exerted control over Gaza. Hamas never exercised actual control over all of Palestine and has agreed – at least in principle – not to disturb the Palestinian Authority, the de jure government of Palestine. Hamas has not declared itself independent from Palestine. Atlantic also does not dispute that Hamas agreed in June 2014 to cede any governing

function it may have had to the Palestinian Authority. As noted by the Congressional Research Service, Hamas has a vested interest in separating its military and political factions. 2010 CRS Hamas Report at 18.

In sum, based on the record before us, Hamas did not constitute a de facto or de jure sovereign during the July 2014 conflict between Hamas and Israel.

[17] **[18]** Our conclusion is bolstered by the executive branch's refusal to recognize Hamas as a de jure or de facto sovereign at the material time. "Who is the sovereign, de jure or de facto, of a territory is ***1159** not a judicial, but is a political question, the determination of which by the legislative and executive departments of any government conclusively binds the judges." *Oetjen v. Cent. Leather Co.*, 246 U.S. 297, 302, 38 S.Ct. 309, 62 L.Ed. 726 (1918). The Supreme Court has held that "recognition of foreign governments so strongly defies judicial treatment that without executive recognition a foreign state has been called 'a republic of whose existence we know nothing,' and the judiciary ordinarily follows the executive as to which nation has sovereignty over disputed territory[.]" *Baker v. Carr*, 369 U.S. 186, 212, 82 S.Ct. 691, 7 L.Ed.2d 663 (1962) (citation omitted). It is only "once sovereignty over an area is politically determined and declared" that "courts may examine the resulting status[.]" *Id.* This court has recognized in the insurance context that "the Constitution commits to the executive branch alone the authority to recognize, and to withdraw recognition from, foreign regimes." *Mingtai Fire & Marine Ins. Co., Ltd. v. United Parcel Serv.*, 177 F.3d 1142, 1145 (9th Cir. 1999). *Mingtai Fire* held that "whether China is the sovereign, de jure or de facto, of the territory of Taiwan is a political question" and thus "we look to the statements and actions of the 'political departments' in order to answer" the question. *Id.*

The executive branch has never recognized Gaza as a state or Hamas as a de jure or de facto sovereign. Instead, pursuant to its authority under § 219 of the INA, 8 U.S.C. § 1189(a)(1), the Secretary of State has consistently designated Hamas as a Foreign Terrorist Organization since 1997. Atlantic does not dispute that the executive branch does not recognize Hamas as a sovereign and instead designates Hamas as a foreign terrorist organization.

Atlantic responds to Universal's arguments about the executive branch by arguing that the definition of "war" in the insurance context under California law "is not a political question to be answered by reference to formal executive or legislative action." Atlantic cites *Ungar v. Palestine Liberation Organization*, 402 F.3d 274, 280 (1st Cir. 2005), which held that a district court's decision regarding sovereignty does not "signal[ ] an official position on behalf of the United States with respect to the political recognition of Palestine." *Ungar* is inapplicable here for two reasons. First, it is non-binding, whereas *Mingtai Fire* is binding on this court. *Mingtai Fire* holds that a court's recognition of sovereignty, even in the insurance context, is a political question. Second, in *Ungar*, the district court declined to recognize Palestine as a state or the Palestinian Authority as a sovereign. The district court's "resolution of that question [was] not incompatible with any formal position thus far taken by the political branches," and thus did not affect the official position of the United States in any manner. *Id.* Here, the district court's analysis – and Atlantic's interpretation – would contradict the executive branch's refusal to recognize Hamas as a sovereign.

Even if the executive branch's position were not per se binding on this court, its position certainly informs our analysis when we face a political question. After considering the factual and historical record and the executive branch's position, we conclude Hamas is not a de jure or a de facto sovereign. Thus, Hamas' conduct in the summer of 2014 cannot be defined as "war" for the purposes of interpreting this policy.

B. The Second War Exclusion

1. *The district court erred in applying "warlike action by a military force" to Hamas' conduct*

[19] **[20]** The district court's interpretation of the second war exclusion, which ***1160** excludes coverage for "warlike action by a military force" by a "government, sovereign, or other authority," is infected by many of the same legal errors as the district court's interpretation of the first exclusion. Like the first exclusion ("war"), the second exclusion ("warlike action") has a special meaning in the insurance industry that derives from the typical exclusion for "warlike operations." *See Pan Am*, 505 F.2d at 1015–17 (analyzing multiple cases holding that "warlike operations" also requires a de jure or a de facto sovereign). That special meaning requires (1) "operations of such a general kind or character as belligerents have recourse to in war," and (2) that such operations be carried out by the military forces of a sovereign or quasi-sovereign government. *See Pan Am World Airways, Inc. v. Aetna Cas. & Sur. Co.*, 368 F. Supp. 1098, 1130

(S.D.N.Y. 1973), *aff'd*, 505 F.2d 989; *see also Holiday Inns*, 571 F. Supp at 1503 (refusing to apply exclusion for "war, invasion, act of foreign enemy, hostilities or *warlike operations* (whether war be declared or not)" to Palestinian and Lebanese sub-national factions' shelling of a Holiday Inn in Beirut (emphasis added)). As with the first exclusion, Atlantic fails to demonstrate how Hamas is a de facto or de jure sovereign and thus engaged in "warlike action by a military force" instead of covered acts of terrorism.

Pan Am distinguished between warlike operations and terrorist activity as follows:

> There is no warrant in the general understanding of English, in history, or in precedent for reading the phrase 'warlike operations' to encompass (1) the infliction of intentional violence by political groups (neither employed by nor representing governments) (2) upon civilian citizens of non-belligerent powers and their property (3) at places far removed from the locale or the subject of any warfare. ... This conclusion is merely reinforced when the evident and avowed purpose of the destructive action is not coercion or conquest in any sense, but the striking of spectacular blows for propaganda effects.

Pan Am, 505 F.2d at 1015–16 (quoting *Pan Am. World Airways, Inc.*, 368 F. Supp. at 1130). A leading insurance treatise notes that "warlike operations" are "normally part of an armed conflict between combatants and usually do not include *intentional violence against civilians by political groups*." 10A Couch on Insurance § 152:3–4 (3d ed. 2017). The treatise also notes that "the standard war exclusion does not explicitly extend to acts of terrorism," as "[t]errorists do not typically fit [the] profile" of "combatants" who "operate lawfully in accordance with the laws and customs of war." *Id.* § 152:18. Atlantic does not provide any evidence to the contrary or explain why warlike operations should cover acts of terrorism.

Atlantic notes that Universal's customary usage for "warlike action" seemingly conflates "war" and "warlike action." Nevertheless, we do not have to identify the precise differences between the two exclusions to conclude that neither exclusion applies here. Customary usage dictates that both exclusions require a showing of de jure or de facto sovereignty, and Atlantic cannot show either. Much of the analysis for the "war" exception applies here.

Moreover, the nature of Hamas' conduct in June and July 2014 also supports our conclusion that Hamas was not engaging in "warlike action by a military force." Couch's insurance treatise notes that "warlike operations" would "not include intentional violence against civilians by political groups." *Id.* § 152:4. Hamas constitutes such a political group. Furthermore, the specific action that disrupted *Dig*'s production was Hamas firing rockets into Israeli civilian centers. One of Universal's experts relied on a U.N. report that determined ***1161** that the weapons Hamas used were unguided missiles and were likely used to injure and kill civilians because of their indiscriminate nature. Hamas' conduct consisted of intentional violence against civilians – conduct which is far closer to acts of terror than "warlike action by a military force."

Because Hamas is not a de facto sovereign – and because its actions did not constitute "warlike action by a military force," – we hold that the second war exclusion does not apply here.

2. *The district court erred in failing to address the efficient proximate cause doctrine in holding Israel indirectly contributed to Hamas' conduct*

[21] In applying the "warlike action" exclusion, the district court concluded that Israel's retaliatory actions also triggered this exclusion. The district court held that "Israel is indisputably a sovereign state, and its actions directly or indirectly contributed to the situation that caused postponement and relocation of the Dig production," as "[i]t is not disputed that Israel took action to counter Hamas' attacks." This conclusion is incorrect for two reasons.

First, even if Israel countered Hamas' attacks, the district court does not explain how Israel's actions were the proximate cause of Universal's losses in moving the production of *Dig*. The evidence indicates that, at the least, Universal's decision to relocate production was a result of Hamas firing rockets into Israel (where filming was occurring), and not a result of Israel's retaliatory conduct.

[22] **[23]** Moreover, the district court's analysis is contrary to California's efficient proximate cause doctrine. "Policy exclusions are unenforceable to the extent that they conflict with section 530 [of the California Insurance Code] and the efficient proximate cause doctrine." *Julian v. Hartford Underwriters Ins. Co.*, 35 Cal.4th 747, 27 Cal.Rptr.3d 648, 110 P.3d 903, 907 (Cal. 2005). The California Supreme Court has held that the "efficient proximate" cause is the "predominant, or most important cause of a loss." *Id.* (citing *Garvey v. State Farm Fire & Cas. Co.*, 48 Cal.3d 395, 257 Cal.Rptr. 292, 770 P.2d 704 (Cal. 1989)). Thus, "the fact that an excluded risk contributed to the loss would not preclude coverage if such a risk was a remote cause of the loss." *Id.*

Here, the record demonstrates that the efficient proximate cause for the relocation was Hamas' rocket fire from Gaza into Israel. The district court's reliance on Israel's indirect contribution to continued hostilities from Hamas was not supported by any evidence in the record. Atlantic's letter denying coverage noted that Universal had to relocate because of "heightened violence in [Israel]" due to Hamas "firing rockets into those cities [Tel Aviv and Jerusalem]" where filming was likely to occur. More importantly, the district court did not consider what the predominant cause of *Dig*'s relocation actually was, and Atlantic provides no evidence that Israeli retaliation was the predominant cause of Universal's losses. The district court erred in holding that because Israel indirectly contributed to Hamas' conduct, Israel's conduct as a sovereign nation triggered the war exclusion here.

Accordingly, we reverse the district court's grant of summary judgment with regard to the second war exclusion.

V. Exclusion Three

Atlantic also asks us to affirm on a ground the district court did not reach: the third exclusion ("insurrection, rebellion, [or] revolution"). As Universal stated at oral argument – and confirmed by the parties' briefing on the motion to strike – this question implicates potential factual ***1162** disputes that the district court has yet to consider. We thus remand to the district court to decide the applicability of the third exclusion in the first instance. [9]

VI. Universal's Bad Faith Claim

Similarly, because we hold that Hamas does not constitute a de jure or de facto sovereign, the policy covers Hamas' hostilities as acts of terrorism creating imminent peril (unless the district court finds that the third exclusion applies). The district court's summary judgment of Universal's bad faith claim was predicated on its erroneous analysis of the first and second war exclusions. Because we reverse the district court's entry of judgment in favor of Atlantic and conclude that Atlantic breached its contract, and because triable issues of fact remain with regard to Universal's claim that Atlantic acted in bad faith in denying its claim, we vacate the district court's judgment on Universal's bad faith claim and remand for further proceedings consistent with our opinion. [10]

VII. Motion to Strike

Atlantic filed a motion to strike portions of Universal's reply brief and further excerpts of the record because Universal relied on materials that were not a part of the district court record (and of which we cannot take judicial notice). These materials were two deposition transcripts that were not filed with the district court, but were filed as further excerpts of the record here. The transcripts involved the third war exclusion, which the district court did not consider.

Because we do not reach the third war exclusion, the motion to strike the portions of the record and reply brief that rely on the unsubmitted materials, *see* Fed. R. App. P. 10; 9th Cir. Rule 30-2, has been mooted.

We decline to sanction Universal for its conduct because the depositions were not scheduled by the parties until after briefing on the summary judgment motion was completed. Universal, thus, did not have an opportunity to supplement the record before this appeal was taken because the district court did not rule on the third war exclusion.

VIII. Conclusion

For the reasons stated above, we hold that Atlantic breached its contract when it denied coverage by defining Hamas' conduct as "war" and "warlike action by a military force." We reverse the district court's entry of summary judgment in favor of Atlantic on the first and second war exclusions, and direct the entry of summary judgment in favor of Universal on the first and second war exclusions. Because the district court did not address the third war exclusion – whether Hamas'

actions constituted "insurrection, rebellion, or revolution" – we remand for the district court to address that question in the first instance. We vacate the grant of summary judgment on Universal's bad faith claim and remand for proceedings consistent with this opinion.

Atlantic's motion to strike [Dkt. 33] is **DENIED** as moot, and the request for sanctions is **DENIED**. Costs on appeal are awarded to Universal.

***1163 REVERSED in part, VACATED in part, and REMANDED with directions.**

All Citations

929 F.3d 1143, 19 Cal. Daily Op. Serv. 6771, 2019 Daily Journal D.A.R. 6527

Footnotes

* The Honorable Ransey Guy Cole, Jr., United States Chief Circuit Judge for the U.S. Court of Appeals for the Sixth Circuit, sitting by designation.

1 The district court did not reach the third war exclusion, i.e., whether Hamas' actions constituted "insurrection, rebellion, or revolution."

2 We rely on the parties' submissions in the record to conduct this brief historical analysis of the conflict.

3 Atlantic argues Hamas began firing rockets in mid-June, but Universal argues it was early July. Because the escalating conduct in early July likely caused Universal to relocate production, July is the relevant time period for our analysis.

4 California courts impute an insurance broker's expertise to its customer/principal. *See Fireman's Fund*, 227 Cal. Rptr. at 206 ("[T]wo large corporate entities, each represented by specialized insurance broker or risk managers, negotiated the terms of the insurance contracts.").

5 The Supreme Court recently addressed California's contra proferentem doctrine in *Lamps Plus, Inc. v. Varela*, —— U.S. ——, 139 S. Ct. 1407, 1417–18, 203 L.Ed.2d 636 (2019). The Court concluded that contra proferentem applies "only after a court determines that it cannot discern the intent of the parties." *Id.* "When a contract is ambiguous, contra proferentem provides a default rule based on public policy." *Id.* We need not address the Supreme Court's discussion of ambiguity because, as noted above, the public policy considerations for applying contra proferentem do not exist here.

6 This requirement ensures that customary usage is not used as a shield against consumers who are entirely unaware of usage in a particular trade.

7 Couch refers to this meaning – requiring sovereignty – as the "ordinary meaning" of war. 10A Couch on Insurance § 152:3 (3d ed. 2017). Couch states that the technical meaning of war in the insurance context requires "formally and constitutionally declared" war. *Id.* Couch does not discuss any other applicable meaning of "war" in the insurance context, including Atlantic's argument for a broader approach.

8 The Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. §§ 9601–9675.

9 Although Atlantic initially raised the fourth exclusion in district court, neither the district court nor the parties on appeal address it. We leave it to the district court to decide whether the fourth exclusion remains a live issue and, if so, to decide its applicability in the first instance.

10 We, of course, recognize and leave open the possibility that how the district court decides the third and fourth exclusions may affect its ultimate decision of Universal's bad faith claim.