




PROGRAM MATERIALS
Program #3063
March 19, 2020

An Overview of NY SHIELD and What You Need to Do to Comply

**Copyright ©2020 by Bradford P. Meisel, Esq. and Diane
D. Reynolds, Esq. - McElroy, Deutsch, Mulvaney &
Carpenter, LLP.
All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

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



An Overview of New York SHIELD and What You Need to do to Comply

CONTINUING LEGAL EDUCATION (CLE)


MARCH 19, 2020


Presenters


- ▶ Diane D. Reynolds, Esq.
 - ▶ Partner; McElroy, Deutsch, Mulvaney & Carpenter, LLP
- ▶ Bradford P. Meisel, Esq.
 - ▶ Associate; McElroy, Deutsch, Mulvaney & Carpenter, LLP





Background and Overview

- 
- ▶ The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act was signed by Gov. Andrew Cuomo (D) on July 25, 2019.
 - ▶ Covered entities are required to be in full compliance by March 21, 2020.
 - ▶ The New York SHIELD Act is the most comprehensive data security law enacted to date in the United States in terms of the specific data security requirements it imposes on covered entities.
 - ▶ The New York SHIELD Act also significantly amended New York's Data Breach Notification Statute.

- 
- ▶ The SHIELD Act was introduced on May 7, 2019 by State Senators Kevin Thomas (D), David Carlucci (D), and Alessandra Biaggi (D). At the request of New York Attorney General Letitia James (D).
 - ▶ A previous version of the SHIELD Act was introduced in 2017 at the request of then-New York Attorney General Eric Schneiderman (D).
 - ▶ The SHIELD Act passed the State Senate by a 41-21 vote on June 17, 2019 and passed the State Assembly by a 47-1 vote the same day.


- 
- ▶ The SHIELD Act broadly defines “private information” subject to the New York Data Breach Notification statute.
 - ▶ The same definition of “private information” applies to the data security provisions of the SHIELD Act.
 - ▶ However, the SHIELD Act narrowed the scope of the information subject to the New York Data Breach Notification statute by amending the statute to only apply to unauthorized access to or acquisition of “private information,” whereas the statute previously applied to “personal information” defined as “any information concerning a natural person, which because of name, number, personal mark, or other identifier,” that “can be used to identify such natural person.”


- 
- ▶ The SHIELD Act defines “private information” as personal information, “any information concerning a natural person, which because of name, number, personal mark, or other identifier, can be used to identify such natural person” in combination with any of the specific types of data listed in the statute if such data is either unencrypted or encrypted with an encryption key that has also been accessed or acquired.


- 
- ▶ The specific types of data enumerated in the SHIELD Act's definition of "private information" are:
 1. Social Security Numbers;
 2. Driver's License or Identification Card Numbers;
 3. Account, Credit Card or Debit Card Numbers (if combined with passwords, codes, or information that permit access or if accounts can be accessed without any additional information, codes, or passwords);
 4. Biometric Information (e.g. fingerprints, iris images, voice prints);
 5. Usernames and Email Addresses (if combined with passwords or security Codes or Questions that would permit access to an online account).





Data Security Provisions


- 
- ▶ The SHIELD Act requires any business or person that owns or licenses data including the private information of New York residents to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of such data.
 - ▶ This provision applies regardless of whether the person or entity does any business in New York or has any physical presence or contacts with New York.
 - ▶ Therefore, any person or entity in the world that possesses the private information of a New York resident is subject to the SHIELD Act.
 - ▶ For example, a small family-owned diner in Omaha, Nebraska could potentially become subject to the SHIELD Act if it possesses the private information of a single customer who resides in New York.


- 
- ▶ The SHIELD Act arguably has broader extraterritorial applicability than some other data security and privacy statutes such as the California Consumer Privacy Act (CCPA), which only applies to entities that “do business in California” or the European Union General Data Protection Regulation (GDPR) which only applies to entities not established in the EU if processing activities relate 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.”
 - ▶ By contrast, simply possessing the data of one New York resident subjects a person or entity to the SHIELD Act in and of itself.


- 
- ▶ The SHIELD Act imposes different data security requirements on small businesses and larger entities.
 - ▶ The SHIELD Act defines a “small business” as a person or business with:
 1. Under 50 employees;
 2. Under \$3 M in gross annual revenue in each of the last 3 fiscal years; or
 3. Less than \$5 M in year-end total assets.


- 
- ▶ The SHIELD Act provides that entities are in full compliance with the statute's data security requirements if they are subject to and in compliance with data security requirements set forth in:
 1. Regulations implementing the Gramm-Leach-Bliley Act;
 2. Regulations implementing HIPAA and the HITECH Act;
 3. NYDFS Regulation Part 500 of Title 23; or
 4. Any other federal or New York data security rules or regulations.


- 
- ▶ The SHIELD Act requires a small business to implement a security program with reasonable administrative, technical, and physical safeguards appropriate for its size and complexity, the nature and scope of its activities, and the sensitivity of the information it collects from customers.
 - ▶ This requirement is similar to proactive cybersecurity statutes enacted in a number of states such as Colorado and Louisiana that require entities that own or license the covered information of state residents to implement reasonable security measures appropriate to the nature of the information and the size of the entity and the nature of its operations.


- 
- ▶ Unlike most other state proactive cybersecurity statutes, such as those in Colorado and Louisiana, the SHIELD Act imposes a number of specific requirements on covered entities too large to constitute small businesses.
 - ▶ These requirements govern such entities' 1) data security programs; 2) reasonable technical safeguards; and 3) reasonable physical safeguards to protect private information from unauthorized access.


- 
- ▶ The SHIELD Act differs from the two most significant data privacy statutes enacted in recent years, namely CCPA and GDPR, as well as a number of pending state privacy bills such as Wisconsin SB 851, Washington SB 6281, and Florida HB 963 are primarily focused on giving consumers specific rights with regard to their personally identifying information unlike the SHIELD Act, which focuses exclusively on requiring persons and entities that possess private information to implement adequate security measures to protect such information from data breaches.


- 
- ▶ The SHIELD Act's data security provisions are not dissimilar from the Insurance Data Security Model Law developed by the National Association of Insurance Commissioners (NAIC), which requires licensed insurers to develop, implement, and maintain information security programs that include risk assessment, assessment of the sufficiency of internal policies and employee training, written incident response plans, and designate an employee to oversee such programs.
 - ▶ Versions of the Model Insurance Data Security Law has been enacted in Michigan, Connecticut, Ohio, South Carolina, New Hampshire, Delaware, Mississippi, and Alabama and legislation to enact versions of it is currently pending in Maine, Oklahoma, Virginia, Illinois, Wisconsin, and Indiana.


- 
- ▶ The required Data Security programs must identify reasonably foreseeable risks including both internal and external threats.
 - ▶ Assessing and mitigating internal threats can be as important if not more important than assessing and mitigating external threats.
 - ▶ For example, a 2018 Verizon study found that 58% of cybersecurity incidents affecting healthcare personal health information (PHI) involved insiders.
 - ▶ In addition to malicious acts, employees can negligently cause cybersecurity incidents by failing to use secure passwords or accessing or downloading content likely to contain malware on enterprise systems.


- 
- ▶ Data Security Programs must include training and managing employees in security program practices and procedures.
 - ▶ In addition to employee training and management, covered entities should strongly consider using content blocking software to ensure employees do not access content or data likely to contain malware such as adult and gaming websites and constantly monitoring employee usage of enterprise systems, networks, and devices to ensure compliance with data security programs and acceptable use policies.

- 
- ▶ Covered entities must designate one or more employees to coordinate their Data Security Programs.
 - ▶ Sizeable entities that possess a significant amount of personally identifying information may be well advised to hire a full time Chief Privacy Officer with significant expertise in data security and privacy regulation to oversee their data security programs and compliance with all potentially applicable data privacy and security laws such as the SHIELD Act as well as CCPA and GDPR.

- 
- ▶ A covered entity's Data Security Program must include assessment of safeguards in place to control identified risks.
 - ▶ Data Security Programs must also include selection of service providers capable of maintaining appropriate safeguards.
 - ▶ Covered entities must contractually require all service providers implement and maintain the safeguards required by the SHIELD Act.
 - ▶ Moreover, covered entities must adjust their Data Security programs in light of business changes or new circumstances.
 - ▶ Therefore, covered entities must follow and develop and implement safeguards to address emerging threats and ensure that they do not create additional vulnerabilities by adopting new technologies such as Cloud Computing or Internet of Things (IoT) connected devices.


- 
- ▶ The SHIELD Act requires covered entities to implement reasonable technological safeguards such as:
 1. Assessing risks in network and software design and information processing, transmission, and storage;
 2. Detecting, preventing and responding to cyberattacks or system failures; and
 3. Regularly testing and monitoring the effectiveness of key controls, systems, and procedures.


- 
- ▶ The SHIELD Act requires covered entities to implement reasonable physical safeguards such as:
 1. Assessing the risks of information storage and disposal;
 2. Detecting, preventing, and responding to intrusions;
 3. Protecting against unauthorized access to use of private information; and
 4. Disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that it cannot be read or reconstructed.

- 
- ▶ Attorneys can position themselves to assist covered entities in effectively and efficiently complying with the SHIELD Act by building and supervising an interdisciplinary team of technical experts to assist clients.
 - ▶ By retaining an interdisciplinary team headed by an attorney rather than a consulting or technology firm, clients can cloak the entire risk assessment, remediation, and compliance process in attorney-client and attorney work-product privilege that can limit discovery in the event of litigation or administrative proceedings or investigations.


- 
- ▶ An interdisciplinary cybersecurity and privacy team headed by an attorney can also overall costs by sharing the expertise of an established team of experts.
 - ▶ Moreover, such an interdisciplinary team can allow for one-stop shopping in which covered entities can have the benefit of a single team capable of providing both technical services and advice as well as legal advice regarding compliance with the SHIELD Act and other data privacy and security laws such as GDPR and CCPA, the legal implications of employee monitoring and management, and navigating the legal and public relations impact of cybersecurity incidents.


- 
- ▶ An interdisciplinary cybersecurity and privacy team headed by an attorney can assist covered entities by:
 1. Developing data security programs and policies that best comply with the SHIELD Act and other potentially applicable statutes and regulations;
 2. Conducting vulnerability assessments and penetration tests;
 3. Conducting due diligence on vendors, hardware, and software;
 4. Drafting SHIELD Act-compliant contracts with service providers;
 5. Weighing the security risks against the benefits of implementing new technologies such as Cloud Computing and IoT connected devices.


- 
- ▶ In the event of a data breach, an interdisciplinary cybersecurity and privacy team headed by an attorney can assist covered entities in:
 1. Complying with all applicable data breach notification statutes and regulations;
 2. Determining whether or not to pay ransom in the event of a ransomware attack;
 3. Proactively managing customer and government relations to potentially reduce the likelihood of litigation, administrative proceedings, and legislative investigations;
 4. Creating an evidentiary record and proactively formulating a defense against potential lawsuits; and
 5. Responding to media, customer, and government inquiries.





Data Breach Notification Provisions


- 
- ▶ The New York Data Breach Notification Statute previously defined a “breach of the security system” subject to notification requirements as unauthorized acquisition of covered data.
 - ▶ The SHIELD Act redefined a “breach of the security system” to include unauthorized access to covered data as well as acquisition of such data.
 - ▶ Connecticut, Florida, and New Jersey are the only other states with data breach notification requirements triggered by unauthorized access to covered data and all other states and the District of Columbia only require notification in the event of unauthorized acquisition of covered data.
 - ▶ However, there is legislation in Wisconsin that would amend the state data breach notification statute to require notification in the event of unauthorized access to covered data.


- 
- ▶ The NY SHIELD Act did not amend the New York Data Breach Notification Statute's requirement that affected individuals as well as the New York Attorney General, Department of State, and State Police be notified "immediately following discovery" of the breach and notify consumer reporting agencies if more than 5,000 New York residents must be notified.
 - ▶ New York is the only state that expressly requires such notice be given "immediately" following discovery of a breach.
 - ▶ Most other state data breach notification statutes require notice without unreasonable delay and as expeditiously as possible and some specify time frames within which notice must be given ranging from 72 hours (California) to 90 days (Connecticut).
 - ▶ Like California, GDPR requires notification within 72 hours.

- 
- ▶ The SHIELD Act provides that in determining if unauthorized access occurred or is reasonably likely to have occurred, a business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by an unauthorized person.
 - ▶ The SHIELD Act left in place pre-existing provisions of the New York Data Breach Notification Statute providing that indicia that a breach has occurred may include lost or stolen computers or devices containing covered information, indications covered information has been downloaded or copied, or reports of identity theft or the opening of fraudulent accounts.

- 
- ▶ The SHIELD Act provides that if a customer's email account can be accessed using information affected by the breach, the required notice must be delivered to the customer when he or she is connected to the account from an IP address or online account the notifying person or entity knows her or she customarily uses to access the account in question.
 - ▶ Similarly, New Jersey Gov. Phil Murphy (D) signed a bill on May 10, 2019 that amended the state data breach notification statute to prohibit required notices from being sent to email accounts subject to the breach.

- 
- ▶ The NY SHIELD Act exempts entities from disclosure requirements if the information was inadvertently exposed by an authorized person and the person or entity determines that it is unlikely to result in misuse of the information and documents that determination for at least 5 years and provides it in writing to the New York Attorney General within 10 days if it affects over 500 New York Residents.
 - ▶ It also exempts entities regulated under the Gramm-Leach-Bliley Act, HIPAA, the New York State Department of Financial Services Regulation (Part 500 of Title 23), and any other federal or New York data security rules and regulations.

- 
- ▶ Although entities regulated under HIPAA are exempt from the New York Data Breach Notification Statute, the SHIELD Act requires that entities required to provide notice of a breach to the Secretary of Health and Human Services (HHS) under HIPAA or the HITECH Act notify the New York Attorney General within 5 days of notifying the Secretary of HHS.
 - ▶ The SHIELD Act requires such entities to provide such notice to the New York Attorney General even if the breach in question did not involve any “private information” for the purposes of the New York Data Beach Notification Statute.

- 
- ▶ The NY SHIELD Act did not amend the provision of the New York State Data Breach Notification Statute which provides that there is no private right of action for violations and the New York State Attorney General has the exclusive authority to bring actions against persons or entities that violate the statute.
 - ▶ A sizeable minority of state data breach statutes expressly create a private right of action for violations including those in California, Illinois, New Jersey, and South Carolina.
 - ▶ Although some courts have held that other state data breach notification statutes that do not expressly provide for a private right of action may provide for one, multiple courts have held that the New York Data Breach Notification statute does not give rise to a private right of action. See, In re Equifax, Inc. Customer Data Security Breach Litigation; Abdale v. North Shore Long Island Jewish Health System, Inc.

Questions



STATE OF NEW YORK

5575--B

Cal. No. 1094

2019-2020 Regular Sessions

IN SENATE

May 7, 2019

Introduced by Sens. THOMAS, CARLUCCI, BIAGGI -- (at request of the Attorney General) -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology -- committee discharged and said bill committed to the Committee on Consumer Protection -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- reported favorably from said committee, ordered to first and second report, ordered to a third reading, passed by Senate and delivered to the Assembly, recalled, vote reconsidered, restored to third reading, amended and ordered reprinted, retaining its place in the order of third reading

AN ACT to amend the general business law and the state technology law, in relation to notification of a security breach

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. This act shall be known and may be cited as the "Stop Hacks
2 and Improve Electronic Data Security Act (SHIELD Act)".

3 § 2. The article heading of article 39-F of the general business law,
4 as added by chapter 442 of the laws of 2005, is amended to read as
5 follows:

6 NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE
7 INFORMATION; DATA SECURITY PROTECTIONS

8 § 3. Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section 899-aa of the
9 general business law, subdivisions 1, 2, 3, 5, 6 and 7 as added by chap-
10 ter 442 of the laws of 2005, paragraph (c) of subdivision 1, paragraph
11 (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the
12 laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6
13 of part N of chapter 55 of the laws of 2013, are amended, subdivision 9
14 is renumbered subdivision 10 and a new subdivision 9 is added to read as
15 follows:

16 1. As used in this section, the following terms shall have the follow-
17 ing meanings:

EXPLANATION--Matter in italics (underscored) is new; matter in brackets
[-] is old law to be omitted.

LBD05343-07-9

1 (a) "Personal information" shall mean any information concerning a
2 natural person which, because of name, number, personal mark, or other
3 identifier, can be used to identify such natural person;

4 (b) "Private information" shall mean either: (i) personal information
5 consisting of any information in combination with any one or more of the
6 following data elements, when either the data element or the combination
7 of personal information [~~or~~] plus the data element is not encrypted, or
8 is encrypted with an encryption key that has also been accessed or
9 acquired:

10 (1) social security number;

11 (2) driver's license number or non-driver identification card number;
12 [~~or~~]

13 (3) account number, credit or debit card number, in combination with
14 any required security code, access code, [~~or~~] password or other informa-
15 tion that would permit access to an individual's financial account;

16 (4) account number, credit or debit card number, if circumstances
17 exist wherein such number could be used to access an individual's finan-
18 cial account without additional identifying information, security code,
19 access code, or password; or

20 (5) biometric information, meaning data generated by electronic meas-
21 urements of an individual's unique physical characteristics, such as a
22 fingerprint, voice print, retina or iris image, or other unique physical
23 representation or digital representation of biometric data which are
24 used to authenticate or ascertain the individual's identity; or

25 (ii) a user name or e-mail address in combination with a password or
26 security question and answer that would permit access to an online
27 account.

28 "Private information" does not include publicly available information
29 which is lawfully made available to the general public from federal,
30 state, or local government records.

31 (c) "Breach of the security of the system" shall mean unauthorized
32 access to or acquisition of, or access to or acquisition without valid
33 authorization, of computerized data that compromises the security,
34 confidentiality, or integrity of [~~personal~~] private information main-
35 tained by a business. Good faith access to, or acquisition of
36 [~~personal~~], private information by an employee or agent of the business
37 for the purposes of the business is not a breach of the security of the
38 system, provided that the private information is not used or subject to
39 unauthorized disclosure.

40 In determining whether information has been accessed, or is reasonably
41 believed to have been accessed, by an unauthorized person or a person
42 without valid authorization, such business may consider, among other
43 factors, indications that the information was viewed, communicated with,
44 used, or altered by a person without valid authorization or by an unau-
45 thorized person.

46 In determining whether information has been acquired, or is reasonably
47 believed to have been acquired, by an unauthorized person or a person
48 without valid authorization, such business may consider the following
49 factors, among others:

50 (1) indications that the information is in the physical possession and
51 control of an unauthorized person, such as a lost or stolen computer or
52 other device containing information; or

53 (2) indications that the information has been downloaded or copied; or

54 (3) indications that the information was used by an unauthorized
55 person, such as fraudulent accounts opened or instances of identity
56 theft reported.

1 (d) "Consumer reporting agency" shall mean any person which, for mone-
2 tary fees, dues, or on a cooperative nonprofit basis, regularly engages
3 in whole or in part in the practice of assembling or evaluating consumer
4 credit information or other information on consumers for the purpose of
5 furnishing consumer reports to third parties, and which uses any means
6 or facility of interstate commerce for the purpose of preparing or
7 furnishing consumer reports. A list of consumer reporting agencies shall
8 be compiled by the state attorney general and furnished upon request to
9 any person or business required to make a notification under subdivision
10 two of this section.

11 2. Any person or business which [~~conducts business in New York state,~~
12 ~~and which~~] owns or licenses computerized data which includes private
13 information shall disclose any breach of the security of the system
14 following discovery or notification of the breach in the security of the
15 system to any resident of New York state whose private information was,
16 or is reasonably believed to have been, accessed or acquired by a person
17 without valid authorization. The disclosure shall be made in the most
18 expedient time possible and without unreasonable delay, consistent with
19 the legitimate needs of law enforcement, as provided in subdivision four
20 of this section, or any measures necessary to determine the scope of the
21 breach and restore the [~~reasonable~~] integrity of the system.

22 (a) Notice to affected persons under this section is not required if
23 the exposure of private information was an inadvertent disclosure by
24 persons authorized to access private information, and the person or
25 business reasonably determines such exposure will not likely result in
26 misuse of such information, or financial harm to the affected persons or
27 emotional harm in the case of unknown disclosure of online credentials
28 as found in subparagraph (ii) of paragraph (b) of subdivision one of
29 this section. Such a determination must be documented in writing and
30 maintained for at least five years. If the incident affects over five
31 hundred residents of New York, the person or business shall provide the
32 written determination to the state attorney general within ten days
33 after the determination.

34 (b) If notice of the breach of the security of the system is made to
35 affected persons pursuant to the breach notification requirements under
36 any of the following laws, nothing in this section shall require any
37 additional notice to those affected persons, but notice still shall be
38 provided to the state attorney general, the department of state and the
39 division of state police pursuant to paragraph (a) of subdivision eight
40 of this section and to consumer reporting agencies pursuant to paragraph
41 (b) of subdivision eight of this section:

42 (i) regulations promulgated pursuant to Title V of the federal Gramm-
43 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

44 (ii) regulations implementing the Health Insurance Portability and
45 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
46 from time to time, and the Health Information Technology for Economic
47 and Clinical Health Act, as amended from time to time;

48 (iii) part five hundred of title twenty-three of the official compila-
49 tion of codes, rules and regulations of the state of New York, as
50 amended from time to time; or

51 (iv) any other data security rules and regulations of, and the stat-
52 utes administered by, any official department, division, commission or
53 agency of the federal or New York state government as such rules, regu-
54 lations or statutes are interpreted by such department, division,
55 commission or agency or by the federal or New York state courts.

1 3. Any person or business which maintains computerized data which
2 includes private information which such person or business does not own
3 shall notify the owner or licensee of the information of any breach of
4 the security of the system immediately following discovery, if the
5 private information was, or is reasonably believed to have been,
6 accessed or acquired by a person without valid authorization.

7 5. The notice required by this section shall be directly provided to
8 the affected persons by one of the following methods:

9 (a) written notice;

10 (b) electronic notice, provided that the person to whom notice is
11 required has expressly consented to receiving said notice in electronic
12 form and a log of each such notification is kept by the person or busi-
13 ness who notifies affected persons in such form; provided further,
14 however, that in no case shall any person or business require a person
15 to consent to accepting said notice in said form as a condition of
16 establishing any business relationship or engaging in any transaction.

17 (c) telephone notification provided that a log of each such notifica-
18 tion is kept by the person or business who notifies affected persons; or

19 (d) substitute notice, if a business demonstrates to the state attor-
20 ney general that the cost of providing notice would exceed two hundred
21 fifty thousand dollars, or that the affected class of subject persons to
22 be notified exceeds five hundred thousand, or such business does not
23 have sufficient contact information. Substitute notice shall consist of
24 all of the following:

25 (1) e-mail notice when such business has an e-mail address for the
26 subject persons, except if the breached information includes an e-mail
27 address in combination with a password or security question and answer
28 that would permit access to the online account, in which case the person
29 or business shall instead provide clear and conspicuous notice delivered
30 to the consumer online when the consumer is connected to the online
31 account from an internet protocol address or from an online location
32 which the person or business knows the consumer customarily uses to
33 access the online account;

34 (2) conspicuous posting of the notice on such business's web site
35 page, if such business maintains one; and

36 (3) notification to major statewide media.

37 6. (a) whenever the attorney general shall believe from evidence
38 satisfactory to him or her that there is a violation of this article he
39 or she may bring an action in the name and on behalf of the people of
40 the state of New York, in a court of justice having jurisdiction to
41 issue an injunction, to enjoin and restrain the continuation of such
42 violation. In such action, preliminary relief may be granted under
43 article sixty-three of the civil practice law and rules. In such action
44 the court may award damages for actual costs or losses incurred by a
45 person entitled to notice pursuant to this article, if notification was
46 not provided to such person pursuant to this article, including conse-
47 quential financial losses. Whenever the court shall determine in such
48 action that a person or business violated this article knowingly or
49 recklessly, the court may impose a civil penalty of the greater of five
50 thousand dollars or up to [~~ten~~] twenty dollars per instance of failed
51 notification, provided that the latter amount shall not exceed [~~one~~] two
52 hundred fifty thousand dollars.

53 (b) the remedies provided by this section shall be in addition to any
54 other lawful remedy available.

55 (c) no action may be brought under the provisions of this section
56 unless such action is commenced within [~~two~~] three years [~~immediately~~]

1 after either the date [~~of the act complained of or the date of discovery~~
2 ~~of such act~~] on which the attorney general became aware of the
3 violation, or the date of notice sent pursuant to paragraph (a) of
4 subdivision eight of this section, whichever occurs first. In no event
5 shall an action be brought after six years from the date of discovery of
6 the breach of private information by the company unless the company took
7 steps to hide the breach.

8 7. Regardless of the method by which notice is provided, such notice
9 shall include contact information for the person or business making the
10 notification, the telephone numbers and websites of the relevant state
11 and federal agencies that provide information regarding security breach
12 response and identity theft prevention and protection information, and a
13 description of the categories of information that were, or are reason-
14 ably believed to have been, accessed or acquired by a person without
15 valid authorization, including specification of which of the elements of
16 personal information and private information were, or are reasonably
17 believed to have been, so accessed or acquired.

18 8. (a) In the event that any New York residents are to be notified,
19 the person or business shall notify the state attorney general, the
20 department of state and the division of state police as to the timing,
21 content and distribution of the notices and approximate number of
22 affected persons and shall provide a copy of the template of the notice
23 sent to affected persons. Such notice shall be made without delaying
24 notice to affected New York residents.

25 (b) In the event that more than five thousand New York residents are
26 to be notified at one time, the person or business shall also notify
27 consumer reporting agencies as to the timing, content and distribution
28 of the notices and approximate number of affected persons. Such notice
29 shall be made without delaying notice to affected New York residents.

30 9. Any covered entity required to provide notification of a breach,
31 including breach of information that is not "private information" as
32 defined in paragraph (b) of subdivision one of this section, to the
33 secretary of health and human services pursuant to the Health Insurance
34 Portability and Accountability Act of 1996 or the Health Information
35 Technology for Economic and Clinical Health Act, as amended from time to
36 time, shall provide such notification to the state attorney general
37 within five business days of notifying the secretary.

38 § 4. The general business law is amended by adding a new section 899-
39 bb to read as follows:

40 § 899-bb. Data security protections. 1. Definitions. (a) "Compliant
41 regulated entity" shall mean any person or business that is subject to,
42 and in compliance with, any of the following data security requirements:

43 (i) regulations promulgated pursuant to Title V of the federal Gramm-
44 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

45 (ii) regulations implementing the Health Insurance Portability and
46 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
47 from time to time, and the Health Information Technology for Economic
48 and Clinical Health Act, as amended from time to time;

49 (iii) part five hundred of title twenty-three of the official compila-
50 tion of codes, rules and regulations of the state of New York, as
51 amended from time to time; or

52 (iv) any other data security rules and regulations of, and the stat-
53 utes administered by, any official department, division, commission or
54 agency of the federal or New York state government as such rules, regu-
55 lations or statutes are interpreted by such department, division,
56 commission or agency or by the federal or New York state courts.

1 (b) "Private information" shall have the same meaning as defined in
2 section eight hundred ninety-nine-aa of this article.

3 (c) "Small business" shall mean any person or business with (i) fewer
4 than fifty employees; (ii) less than three million dollars in gross
5 annual revenue in each of the last three fiscal years; or (iii) less
6 than five million dollars in year-end total assets, calculated in
7 accordance with generally accepted accounting principles.

8 2. Reasonable security requirement. (a) Any person or business that
9 owns or licenses computerized data which includes private information of
10 a resident of New York shall develop, implement and maintain reasonable
11 safeguards to protect the security, confidentiality and integrity of the
12 private information including, but not limited to, disposal of data.

13 (b) A person or business shall be deemed to be in compliance with
14 paragraph (a) of this subdivision if it either:

15 (i) is a compliant regulated entity as defined in subdivision one of
16 this section; or

17 (ii) implements a data security program that includes the following:

18 (A) reasonable administrative safeguards such as the following, in
19 which the person or business:

20 (1) designates one or more employees to coordinate the security
21 program;

22 (2) identifies reasonably foreseeable internal and external risks;

23 (3) assesses the sufficiency of safeguards in place to control the
24 identified risks;

25 (4) trains and manages employees in the security program practices and
26 procedures;

27 (5) selects service providers capable of maintaining appropriate safe-
28 guards, and requires those safeguards by contract; and

29 (6) adjusts the security program in light of business changes or new
30 circumstances; and

31 (B) reasonable technical safeguards such as the following, in which
32 the person or business:

33 (1) assesses risks in network and software design;

34 (2) assesses risks in information processing, transmission and stor-
35 age;

36 (3) detects, prevents and responds to attacks or system failures; and

37 (4) regularly tests and monitors the effectiveness of key controls,
38 systems and procedures; and

39 (C) reasonable physical safeguards such as the following, in which the
40 person or business:

41 (1) assesses risks of information storage and disposal;

42 (2) detects, prevents and responds to intrusions;

43 (3) protects against unauthorized access to or use of private informa-
44 tion during or after the collection, transportation and destruction or
45 disposal of the information; and

46 (4) disposes of private information within a reasonable amount of time
47 after it is no longer needed for business purposes by erasing electronic
48 media so that the information cannot be read or reconstructed.

49 (c) A small business as defined in paragraph (c) of subdivision one of
50 this section complies with subparagraph (ii) of paragraph (b) of subdi-
51 vision two of this section if the small business's security program
52 contains reasonable administrative, technical and physical safeguards
53 that are appropriate for the size and complexity of the small business,
54 the nature and scope of the small business's activities, and the sensi-
55 tivity of the personal information the small business collects from or
56 about consumers.

1 (d) Any person or business that fails to comply with this subdivision
2 shall be deemed to have violated section three hundred forty-nine of
3 this chapter, and the attorney general may bring an action in the name
4 and on behalf of the people of the state of New York to enjoin such
5 violations and to obtain civil penalties under section three hundred
6 fifty-d of this chapter.

7 (e) Nothing in this section shall create a private right of action.

8 § 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8
9 of section 208 of the state technology law, paragraph (a) of subdivision
10 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005,
11 subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5
12 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as
13 amended by chapter 491 of the laws of 2005, are amended and a new subdi-
14 vision 9 is added to read as follows:

15 (a) "Private information" shall mean either: (i) personal information
16 consisting of any information in combination with any one or more of the
17 following data elements, when either the data element or the combination
18 of personal information [~~or~~] plus the data element is not encrypted or
19 encrypted with an encryption key that has also been accessed or
20 acquired:

21 (1) social security number;

22 (2) driver's license number or non-driver identification card number;
23 [~~or~~]

24 (3) account number, credit or debit card number, in combination with
25 any required security code, access code, [~~or~~] password or other informa-
26 tion which would permit access to an individual's financial account;

27 (4) account number, or credit or debit card number, if circumstances
28 exist wherein such number could be used to access to an individual's
29 financial account without additional identifying information, security
30 code, access code, or password; or

31 (5) biometric information, meaning data generated by electronic meas-
32 urements of an individual's unique physical characteristics, such as
33 fingerprint, voice print, or retina or iris image, or other unique phys-
34 ical representation or digital representation which are used to authen-
35 ticate or ascertain the individual's identity; or

36 (ii) a user name or e-mail address in combination with a password or
37 security question and answer that would permit access to an online
38 account.

39 "Private information" does not include publicly available information
40 that is lawfully made available to the general public from federal,
41 state, or local government records.

42 2. Any state entity that owns or licenses computerized data that
43 includes private information shall disclose any breach of the security
44 of the system following discovery or notification of the breach in the
45 security of the system to any resident of New York state whose private
46 information was, or is reasonably believed to have been, accessed or
47 acquired by a person without valid authorization. The disclosure shall
48 be made in the most expedient time possible and without unreasonable
49 delay, consistent with the legitimate needs of law enforcement, as
50 provided in subdivision four of this section, or any measures necessary
51 to determine the scope of the breach and restore the [~~reasonable~~] integ-
52 rity of the data system. The state entity shall consult with the state
53 office of information technology services to determine the scope of the
54 breach and restoration measures. Within ninety days of the notice of the
55 breach, the office of information technology services shall deliver a

1 report on the scope of the breach and recommendations to restore and
2 improve the security of the system to the state entity.

3 (a) Notice to affected persons under this section is not required if
4 the exposure of private information was an inadvertent disclosure by
5 persons authorized to access private information, and the state entity
6 reasonably determines such exposure will not likely result in misuse of
7 such information, or financial or emotional harm to the affected
8 persons. Such a determination must be documented in writing and main-
9 tained for at least five years. If the incident affected over five
10 hundred residents of New York, the state entity shall provide the writ-
11 ten determination to the state attorney general within ten days after
12 the determination.

13 (b) If notice of the breach of the security of the system is made to
14 affected persons pursuant to the breach notification requirements under
15 any of the following laws, nothing in this section shall require any
16 additional notice to those affected persons, but notice still shall be
17 provided to the state attorney general, the department of state and the
18 office of information technology services pursuant to paragraph (a) of
19 subdivision seven of this section and to consumer reporting agencies
20 pursuant to paragraph (b) of subdivision seven of this section:

21 (i) regulations promulgated pursuant to Title V of the federal Gramm-
22 Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

23 (ii) regulations implementing the Health Insurance Portability and
24 Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended
25 from time to time, and the Health Information Technology for Economic
26 and Clinical Health Act, as amended from time to time;

27 (iii) part five hundred of title twenty-three of the official compila-
28 tion of codes, rules and regulations of the state of New York, as
29 amended from time to time; or

30 (iv) any other data security rules and regulations of, and the stat-
31 utes administered by, any official department, division, commission or
32 agency of the federal or New York state government as such rules, regu-
33 lations or statutes are interpreted by such department, division,
34 commission or agency or by the federal or New York state courts.

35 3. Any state entity that maintains computerized data that includes
36 private information which such agency does not own shall notify the
37 owner or licensee of the information of any breach of the security of
38 the system immediately following discovery, if the private information
39 was, or is reasonably believed to have been, accessed or acquired by a
40 person without valid authorization.

41 6. Regardless of the method by which notice is provided, such notice
42 shall include contact information for the state entity making the
43 notification, the telephone numbers and websites of the relevant state
44 and federal agencies that provide information regarding security breach
45 response and identity theft prevention and protection information and a
46 description of the categories of information that were, or are reason-
47 ably believed to have been, accessed or acquired by a person without
48 valid authorization, including specification of which of the elements of
49 personal information and private information were, or are reasonably
50 believed to have been, so accessed or acquired.

51 7. (a) In the event that any New York residents are to be notified,
52 the state entity shall notify the state attorney general, the department
53 of state and the state office of information technology services as to
54 the timing, content and distribution of the notices and approximate
55 number of affected persons and provide a copy of the template of the

1 notice sent to affected persons. Such notice shall be made without
2 delaying notice to affected New York residents.

3 (b) In the event that more than five thousand New York residents are
4 to be notified at one time, the state entity shall also notify consumer
5 reporting agencies as to the timing, content and distribution of the
6 notices and approximate number of affected persons. Such notice shall be
7 made without delaying notice to affected New York residents.

8 8. The state office of information technology services shall develop,
9 update and provide regular training to all state entities relating to
10 best practices for the prevention of a breach of the security of the
11 system.

12 9. Any covered entity required to provide notification of a breach,
13 including breach of information that is not "private information" as
14 defined in paragraph (a) of subdivision one of this section, to the
15 secretary of health and human services pursuant to the Health Insurance
16 Portability and Accountability Act of 1996 or the Health Information
17 Technology for Economic and Clinical Health Act, as amended from time to
18 time, shall provide such notification to the state attorney general
19 within five business days of notifying the secretary.

20 10. Any entity listed in subparagraph two of paragraph (c) of subdi-
21 vision one of this section shall adopt a notification policy no more
22 than one hundred twenty days after the effective date of this section.
23 Such entity may develop a notification policy which is consistent with
24 this section or alternatively shall adopt a local law which is consist-
25 ent with this section.

26 § 6. This act shall take effect on the ninetieth day after it shall
27 have become a law; provided, however, that section four of this act
28 shall take effect on the two hundred fortieth day after it shall have
29 become a law.



KeyCite Yellow Flag - Negative Treatment

Disagreed With by [Fero v. Excellus Health Plain, Inc.](#), W.D.N.Y., February 22, 2017

49 Misc.3d 1027

Supreme Court, Queens County, New York.

Denise R. ABDALE, Helene Butler, Paulette Schramm, Charleen Solomon, Lena Vetere, [Charles Billups](#), Diane Peterman, M.D., [Katherine Cross](#), Linda Kiehl, Elizabeth Caporaso, Richard Ertl and Jarrett Akins, on behalf of themselves and all others similarly situated, Plaintiff,

v.

NORTH SHORE–LONG ISLAND JEWISH HEALTH SYSTEM, INC., North Shore–Long Island Jewish Medical Care, PLLC, North Shore–Lij Network, Inc. and North Shore University Hospital, Defendant.

Aug. 14, 2015.

Synopsis

Background: Patients brought action against health care facilities after their confidential personal and medical information was stolen by a third party, and action was removed to federal court. The United States District Court for the Eastern District of New York remanded the case, and defendants moved to dismiss.

Holdings: The Supreme Court, Queens County, Robert J. McDonald, J., held that:

[1] statute requiring businesses that own or license computerized data to notify state residents of the unauthorized acquisition of their private information did not create implied private right of action;

[2] theft of personal and health information contained in defendants' data base was not a disclosure of such information under statute limiting access to patient information;

[3] no private right of action exists with respect to a violation of statute instituting safeguards necessary to thwart unauthorized access to social security numbers;

[4] defendants' alleged failure to safeguard patients' protected health information and identifying information from theft did not constitute a deceptive practice within meaning of the deceptive trade practices statute;

[5] patients failed to state claim for breach of contract;

[6] patients allegations stated negligence claim against some of the defendants; and

[7] fraud claims could not be made collectively against all defendants.

Ordered accordingly.

West Headnotes (28)

[1] Pretrial Procedure

🔑 Construction of pleadings

Pretrial Procedure

🔑 Presumptions and burden of proof

On a motion to dismiss for failure to state a cause of action, the complaint must be construed liberally, the factual allegations deemed to be true, and the nonmoving party must be given the benefit of all favorable inferences. [McKinney's CPLR 3211\(a\)\(7\)](#).

[2] Pretrial Procedure

🔑 Matters considered in general

On a motion to dismiss for failure to state a cause of action, the court is limited to an examination of the pleadings to determine whether they state a cause of action, and the plaintiff may not be penalized for failure to make an evidentiary showing in support of a complaint that states a claim on its face.

[3] Pretrial Procedure

🔑 Insufficiency in general

Pretrial Procedure

🔑 Availability of relief under any state of facts provable

The test of the sufficiency of a pleading is whether it gives sufficient notice of the transactions, occurrences, or series of transactions or occurrences intended to be proved and whether the requisite elements of any cause of action known to the law can be discerned from its averments. [McKinney's CPLR 3211\(a\)\(7\)](#).

[4] Pretrial Procedure

🔑 Evidence

A court is permitted to consider evidentiary material in support of a motion to dismiss for failure to state a cause of action, and, if it does so, the criterion then becomes whether the proponent of the pleading has a cause of action, not whether he has stated one. [McKinney's CPLR 3211\(a\)\(7\)](#).

[5] Pretrial Procedure

🔑 Fact questions

A motion to dismiss for failure to state a cause of action must be denied unless it has been shown that a material fact as claimed by the pleader to be one is not a fact at all and unless it can be said that no significant dispute exists regarding it. [McKinney's CPLR 3211\(a\)\(7\)](#).

[6] Action

🔑 Statutory rights of action

Antitrust and Trade Regulation

🔑 Public entities or officials

Antitrust and Trade Regulation

🔑 Private entities or individuals

Statute requiring businesses that own or license computerized data to notify state residents of the unauthorized acquisition of their private information did not create implied private right of action; statute expressly provided for enforcement by the attorney general. [McKinney's General Business Law § 899-aa](#).

1 Cases that cite this headnote

[7] Action

🔑 Statutory rights of action

In the absence of an express private right of action, plaintiffs can seek civil relief in a plenary action based on a violation of a statute only if a legislative intent to create such a right of action is fairly implied in the statutory provisions and their legislative history.

1 Cases that cite this headnote

[8] Action

🔑 Statutory rights of action

Determination of whether a statute creates an implied private right of action is predicated on three factors: (1) whether the plaintiff is one of the class for whose particular benefit the statute was enacted; (2) whether recognition of a private right of action would promote the legislative purpose; and (3) whether creation of such a right would be consistent with the legislative scheme.

1 Cases that cite this headnote

[9] Action

🔑 Statutory rights of action

Regardless of its consistency with the basic legislative goal, a private right of action should not be judicially sanctioned if it is incompatible with the enforcement mechanism chosen by the Legislature or with some other aspect of the overall statutory scheme.

[10] Health

🔑 Confidentiality; patient records

Theft of personal and health information contained in health care facilities' data base was not a disclosure of such information under statute limiting access to patient information, where the providers were not participants in the data theft. [McKinney's Public Health Law § 18](#).

[11] Action

🔑 Statutory rights of action

Health

🔑 [Records and duty to report; confidentiality in general](#)

Alleged unauthorized disclosure of patients' medical records as result of data theft did not give rise to private cause of action against health care providers under statute limiting access to patient information. [McKinney's Public Health Law § 18](#).

[12] Action

🔑 [Statutory rights of action](#)

Antitrust and Trade Regulation

🔑 [Private entities or individuals](#)

As enforcement of provisions of statute instituting safeguards necessary to thwart unauthorized access to social security numbers have been entrusted to the attorney general, no private right of action exists with respect to a violation of the statute. [McKinney's General Business Law § 399–ddd\(4\)](#).

[13] Action

🔑 [Statutory rights of action](#)

Health

🔑 [Records and duty to report; confidentiality in general](#)

HIPPA and its regulations do not create a private right of action. Health Insurance Portability and Accountability Act of 1996, 1(a), [42 U.S.C.A. § 201](#) note.

[14] Action

🔑 [Statutory rights of action](#)

Health

🔑 [Records and duty to report; confidentiality in general](#)

Neither Health Information Technology for Economic and Clinical Health Act (HITECH), providing for privacy and security of patient health information, nor its governing regulations create a private right of action. Health Information Technology for Economic and Clinical Health Act, Div. A, Title XIII, § 13400, [42 U.S.C.A. § 17921](#).

[15] Antitrust and Trade Regulation

🔑 [In general; unfairness](#)

A prima facie case under the deceptive trade practices statute requires a showing that the defendant engaged in a consumer-oriented act or practice that was deceptive or misleading in a material way and that the plaintiff has been injured by reason thereof. [McKinney's General Business Law § 349\(h\)](#).

[16] Antitrust and Trade Regulation

🔑 [Privacy](#)

Medical facilities' alleged failure to safeguard patients' protected health information and identifying information from theft did not misled the patients in any material way and did not constitute a deceptive practice within the meaning of the deceptive trade practices statute. [McKinney's General Business Law § 349\(h\)](#).

[1 Cases that cite this headnote](#)

[17] Contracts

🔑 [Grounds of action](#)

The essential elements of a cause of action to recover damages for breach of contract are the existence of a contract, the plaintiff's performance pursuant to the contract, the defendant's breach of its contractual obligations, and damages resulting from the breach.

[1 Cases that cite this headnote](#)

[18] Contracts

🔑 [Allegation or Statement of Contract or Promise](#)

A complaint must plead the provisions of the contract upon which the cause of action for breach of contract is based.

[1 Cases that cite this headnote](#)

[19] Health

🔑 [Confidentiality; patient records](#)

Patients' allegations that they provided personal information to various medical facilities, which were contractually obligated to protect their private health and personal information, and that the facilities breached their contractual obligations by permitting or inadequately protecting against theft of such information were insufficient to state claim against the facilities for breach of contract; patients failed to allege that they each had a contractual relationship with each of the facilities, and failed to allege any specific provision that the facilities allegedly breached, or that any privacy statement contained an obligation or promise regarding theft of personal information by third parties.

[1 Cases that cite this headnote](#)

[20] Fraud

🔑 Fiduciary or confidential relations

Elements of a cause of action to recover damages for breach of fiduciary duty are (1) the existence of a fiduciary relationship, (2) misconduct by the defendant, and (3) damages directly caused by the defendant's misconduct.

[21] Pleading

🔑 Certainty, definiteness, and particularity

A claim for breach of fiduciary duty must be pleaded with particularity, and the circumstances constituting the alleged wrong must be stated in detail. [McKinney's CPLR 3016\(b\)](#).

[22] Negligence

🔑 Elements in general

To establish a prima facie case of negligence, a plaintiff must establish the existence of a duty owed by a defendant to the plaintiff, a breach of that duty, and that such breach was the proximate cause of injury to the plaintiff.

[23] Health

🔑 Confidentiality; patient records

Patients' allegations that they gave personal information to treating facilities in order to

receive medical treatment, that the facilities informed them that their personal information would not be disclosed to third parties without their consent, and that an employee or employees of the facilities stole their personal information and sold it to third parties who used the information to open fraudulent credit card accounts, make fraudulent purchases, and fraudulently obtain income tax returns were sufficient to state negligence claim against the facilities.

[24] Contracts

🔑 Grounds of action

A claim for breach of the duty of good faith and fair dealing may not be used as a substitute for a nonviable claim of breach of contract.

[25] Pleading

🔑 Particular causes of action

Patients' fraud allegations against medical facilities that allegedly failed to timely disclose that their private financial identity, health identity and personal information had been stolen could not be made collectively as to all defendants. [McKinney's CPLR 3016\(b\)](#).

[26] Fraud

🔑 Elements of Actual Fraud

The elements of a cause of action sounding in fraud are a material misrepresentation of an existing fact, made with knowledge of the falsity, an intent to induce reliance thereon, justifiable reliance upon the misrepresentation, and damages.

[27] Fraud

🔑 Duty to disclose facts

A cause of action to recover damages for fraudulent concealment requires, in addition to allegations of scienter, reliance, and damages, an allegation that the defendant had a duty to disclose material information and that it failed to do so.

[28] Fraud

🔑 Allegations of fraud in general

Pleading

🔑 Certainty, definiteness, and particularity

A fraud claim asserted against multiple defendants must include specific and separate allegations for each defendant. [McKinney's CPLR 3016\(b\)](#).

Attorneys and Law Firms

****853** Law Offices of Bonita Zelman, Lake Success, for plaintiffs.

Ropes & Gray, LLP, New York City ([Jason Brown](#) and [Joseph G. Cleemann](#) of counsel), for defendants.

Opinion

ROBERT J. McDONALD, J.

This motion is determined as follows:

1030** Plaintiffs commenced the within action on behalf of themselves and others similarly situated on February 5, 2013 to recover damages for, among other things, defendants' "failure to adequately protect the confidential personal and medical ***1031** information of their current and former patients, conduct that ultimately resulted in identity and medical identity data breaches". Plaintiffs are thirteen patients, or relatives *854** of patients, who allegedly received medical services at medical facilities owned or operated by defendants North Shore–Long Island Jewish Health System, Inc. (Health System), North Shore–Long Island Jewish Medical Care, PLLC, (Medical Care), North Shore–LIJ Network, Inc. (Network) and North Shore University Hospital (NSUH). Plaintiffs allege that defendants Health System, Medical Care and NSUH each operate under the corporate umbrella of defendant Network; and that defendants Network, Health System and Medical Care own, operate, manages, maintains and secures defendant NSUH. The complaint refers to all four defendants collectively as North–Shore LIJ.

Plaintiffs allege that at the time they received medical treatment they provided personal information to the defendants, and that on or before Fall 2010 and continuing at least through 2012, medical record Face Sheets and unencrypted computer network data were stolen from defendants North–Shore LIJ. It is also alleged that patient's physical (hard copy) hospital Face Sheets were unsecured and were stolen from inside the premises of the defendants' facilities, including NSUH. These Face Sheets consist of cover sheets containing information about each patient, including their full name, their spouse's full name if married, date of birth, address, telephone number, medical record number, Social Security number, insurance information, and current medical information and history. Plaintiffs allege that the stolen data contains private, personal information, including but not limited to protected health information as defined by HIPPA, Social Security numbers, medical information and other information of hundreds of patients. Plaintiffs allege that as a result of the defendants' failure to implement and follow basic security procedures, their personal information is now in the hands of thieves, and that they face a substantial increased risk of identity theft. Each of the thirteen plaintiffs allege that they have experienced repeated instances of identity theft since said data breach and as that a consequence of said breach, plaintiffs, as well as current and former patients, have had to spend and will continue to spend significant time and money in the future to protect themselves. In addition, plaintiff Peterman alleges that as a result of the data breach her credit rating was substantially damaged; plaintiff Vetere alleges that as a result of the data breach her ***1032** income tax refund for 2010 was fraudulently claimed and sent to a third party; and plaintiff Akins alleges that identity thieves fraudulently filed state and federal income tax returns for 2011, causing him substantial financial losses.

The complaint alleges that Health System through its Patients' Bill of Rights, and website, advised patients that it, and each of its owned or sponsored Article 28 not-for-profit corporations are required by law to follow HIPPA regulations and protect the privacy of health information that may reveal a patient's identity. The complaint further alleges that patients were also advised that they have a right to be notified of any breaches of "Unsecured Protected Health" information as soon as possible, but in any event no later than 60 days following the discovery of the breaches.

Plaintiffs allege that on January 26, 2012, Clincy M. Robinson was arrested and charged with Identity Theft in the First

Degree (one count) and Criminal Possession of Computer Related Materials (two counts), Scheme to Defraud in the First Degree (2 counts) and Unlawful Possession of Personal Information in the Third Degree (1 count). Mr. Robinson was charged with being in possession of 25 Face Sheets **855 from NSUH, data that is maintained on the computer network of NSUH, and being in possession of computer data consisting of personal identifying information for over 900 individuals, without authorization, and it is alleged that he pled guilty to these charges and was sentenced on December 13, 2012 in the District Court of Nassau County.

Plaintiffs also alleges that on June 1, 2012, Dennis Messias was arrested and charged with Identity Theft in the First Degree (four counts), Grand Larceny in the Third Degree, and Scheme to Defraud in the First Degree, in connection with the theft and unauthorized use of patients' personal information from the premises of NSUH.

Plaintiffs allege that the defendants were aware of these thefts and security breaches and that they failed to notify its patients within 60 days of the breach; that defendants failed to notify the Secretary of the U.S. Department of Health and Human Services of said security breaches in the year in which they discovered said breaches; and that defendants failed to maintain a written log of security breaches since 2007, on an annual basis.

The complaint alleges eleven causes of action for (1) negligence per se based upon violations of [General Business Law § 899–aa](#); *1033 (2) negligence per se based on violations of [Public Health Law § 18](#); (3) negligence per se based upon violations of [General Business Law § 399–dd\(4\)](#); (4) negligence per se based on violations of the Health Insurance Portability and Accountability Act of 1996 (HIPPA), [Pub.L. No. 104–191, 110 Stat.1936 \(1996\)](#); (5) negligence per se based on violations of the Health Information Technology for Economic and Clinical Health Act (HITECH), [42 U.S.C. § 17921–53](#); (6) violations of [General Business Law § 349](#); (7) breach of contract; (8) breach of fiduciary duty; (9) negligence; (10) breach of the implied covenant of good faith and fair dealing; and (11) misrepresentation.

Defendants, prior to serving an answer, filed a notice of removal on March 8, 2013, which removed this action to the United States District Court for the Eastern District of New York (District Court), asserting that a federal jurisdiction question existed and that removal was appropriate under

the Class Action Fairness Act of 2005(CAFA). On April 16, 2013, the defendants filed a motion in District Court to dismiss the complaint and on June 10, 2013, plaintiffs filed a motion to remand the matter to this court. The District Court, in an order dated June 14, 2014, denied the plaintiffs' motion to remand with leave to renew 30 days after the conclusion of expedited discovery pertaining to CAFA exceptions, and reserved judgment on the defendants' motion to dismiss (*Abdale, et al. v. North Shore–Long Island Jewish Health System, Inc., et al.*, 2014 U.S. Dist Lexis 88881 [United States District Court for the Eastern District of New York, 2014]). The parties were unable to formulate a joint discovery plan as directed by the court, and the matter was assigned to a magistrate. A status conference was held on October 2, 2014, at which time the magistrate made certain rulings pertaining to discovery. However, no discovery was had and defendants conceded that the matter should be remanded to this court, as the 268 individuals they sent letters to regarding the subject data breach were all New York State citizens. On November 13, 2014, the District Court remanded the matter back to this court, without any limit as to the size of the class.

Defendants, in this pre-answer motion seek to dismiss the complaint on the grounds of failure to state a cause of action, pursuant to [CPLR 3211\(a\)\(7\)](#).

**856 [1] [2] [3] It is well settled that “[o]n a motion to dismiss pursuant to [CPLR 3211\(a\)\(7\)](#) for failure to state a cause of action, the *1034 complaint must be construed liberally, the factual allegations deemed to be true, and the nonmoving party must be given the benefit of all favorable inferences” (*Leon v. Martinez*, 84 N.Y.2d 83, 87, 614 N.Y.S.2d 972, 638 N.E.2d 511 [1994]; *see AG Capital Funding Partners, L.P. v. State St. Bank & Trust Co.*, 5 N.Y.3d 582, 591, 808 N.Y.S.2d 573, 842 N.E.2d 471 [2005]; *Goshen v. Mutual Life Ins. Co. of NY*, 98 N.Y.2d 314, 326, 746 N.Y.S.2d 858, 774 N.E.2d 1190 [2002]; *Nasca v. Sgro*, 130 A.D.3d 588, 13 N.Y.S.3d 188 [2d Dept.2015]; *Dolphin Holdings, Ltd. v. Gander & White Shipping, Inc.*, 122 A.D.3d 901, 901–902, 998 N.Y.S.2d 107 [2d Dept.2014]). The court is limited to “an examination of the pleadings to determine whether they state a cause of action,” and the “plaintiff may not be penalized for failure to make an evidentiary showing in support of a complaint that states a claim on its face” (*Migliano v. Bally Total Fitness of Greater N.Y., Inc.*, 20 N.Y.3d 342, 351, 961 N.Y.S.2d 364, 985 N.E.2d 128 [2013]). “The test of the sufficiency of a pleading is whether it gives sufficient notice of the transactions, occurrences, or series of transactions or occurrences intended to be proved and

whether the requisite elements of any cause of action known to our law can be discerned from its averments' ” (*V. Groppa Pools, Inc. v. Massello*, 106 A.D.3d 722, 723, 964 N.Y.S.2d 563 [2d Dept.2013], quoting *Pace v. Perk*, 81 A.D.2d 444, 449, 440 N.Y.S.2d 710[2d Dept.1981] [internal quotation marks omitted]; see also *Dolphin Holdings, Ltd. v. Gander & White Shipping, Inc.*, 122 A.D.3d at 901–902, 998 N.Y.S.2d 107).

[4] [5] “A court is, of course, permitted to consider evidentiary material ... in support of a motion to dismiss pursuant to CPLR 3211(a)(7)” (*Sokol v. Leader*, 74 A.D.3d 1180, 1181, 904 N.Y.S.2d 153 [2d Dept.2010]), and, if it does so, “the criterion then becomes whether the proponent of the pleading has a cause of action, not whether he has stated one’ ” (*id.* at 1181–1182, 904 N.Y.S.2d 153, quoting *Guggenheimer v. Ginzburg*, 43 N.Y.2d at 275, 401 N.Y.S.2d 182, 372 N.E.2d 17). “Yet, affidavits submitted by a defendant will almost never warrant dismissal under CPLR 3211 unless they establish conclusively that [the plaintiff] has no cause of action” (*Dolphin Holdings, Ltd. v. Gander & White Shipping, Inc.*, 122 A.D.3d at 902, 998 N.Y.S.2d 107 [internal quotation marks omitted]; see *Bokhour v. GTI Retail Holdings, Inc.*, 94 A.D.3d 682, 941 N.Y.S.2d 675 [2d Dept.2012]). “Indeed, a motion to dismiss pursuant to CPLR 3211(a)(7) must be denied unless it has been shown that a material fact as claimed by the pleader to be one is not a fact at all and unless it can be said that no significant dispute exists *1035 regarding it” (*Bokhour v. GTI Retail Holdings, Inc.*, 94 A.D.3d at 683, 941 N.Y.S.2d 675 [internal quotation marks omitted]; see *Sokol v. Leader*, 74 A.D.3d at 1182, 904 N.Y.S.2d 153; see also *Nasca v. Sgro*, *supra*).

Defendants assert that defendant Health System is a not-for-profit corporation that indirectly owns or sponsors a large number of separate not-for-profit health care providers, including sixteen acute care hospitals; that defendant Medical Care and defendant Network are affiliated with defendant Health System but do not provide any patient services; and that defendant NSUH is one of said sixteen hospitals and is the only defendant that provides direct patient services. It is asserted that the complaint fails to allege any facts with respect to defendants Health System, Medical Care and Network; that plaintiffs do not allege that **857 records were stolen from these entities or that they were a patient of these entities. It is further asserted that the complaint fails to contain any specific factual allegations with respect to these three defendants and that plaintiffs seek to rely upon bald assertions that each of these defendants

operate under the same “corporate umbrella” and each “owns, operates, maintains and secures” defendant NSUH. As regards defendant Network, it is asserted that the complaint appears to state in conclusory fashion that employees of that entity were responsible for the theft of certain personal information.

Defendants assert that the complaint fails to satisfy New York's pleading standards in that the allegations are conclusory; that the complaint fails to assert facts to support any claim against defendants Health System, Medical Care and Network; that the complaint fails to allege cognizable injuries; that the claims of negligence and negligence per se are barred by the economic loss doctrine; that each of the negligence per se claims fail to allege the elements of the alleged statutory violation on which the claim is based; that the claim fails to allege the elements of misrepresentation, whether framed as a common law violation or an alleged deceptive practice under *General Business Law* § 349; that the complaint fails to allege the elements of breach of contract and breach of the implied covenant of good faith and fair dealing; and that the complaint fails to allege the core elements necessary to support a claim of breach of fiduciary duty.

CPLR 1303 requires that “[s]tatements in a pleading shall be sufficiently particular to give the court and the parties notice of the transactions, occurrences, or series of transactions or occurrences, *1036 intended to be proved and the material elements of each cause of action or defense”.

[6] The first cause of action for negligence per se is based upon *General Business Law* § 899–aa. Said statute provides that any person or business which conducts business in New York state and owns or licenses computerized data which includes certain private information is required to disclose any breach of the security of the system to any resident of New York state “whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.” The statute sets forth the time frame and method of giving such notice. Reviewing said statute in a light most favorable to the plaintiffs, it is clear that there is no private right of action expressly authorized pursuant to the statute. Rather, said statute expressly provides at subsection 6 that the attorney general may bring an action for a violation of said statute, and further provides that in such an action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to said article.

[7] [8] [9] In the absence of an express private right of action, plaintiffs can seek civil relief in a plenary action based on a violation of the statute “only if a legislative intent to create such a right of action is fairly implied in the statutory provisions and their legislative history” (*Carrier v. Salvation Army*, 88 N.Y.2d 298, 302, 644 N.Y.S.2d 678, 667 N.E.2d 328 [1996] [internal quotation marks and citations omitted]). This determination is predicated on three factors: “(1) whether the plaintiff is one of the class for whose particular benefit the statute was enacted; (2) whether recognition of a private right of action would promote the legislative purpose; and (3) whether creation of such a right would be consistent with the legislative scheme” (*Sheehy v. Big Flats Community Day*, 73 N.Y.2d 629, 633, 543 N.Y.S.2d 18, 541 N.E.2d 18 [1989]). The Court of Appeals **858 has repeatedly recognized the third as the most important because “the Legislature has both the right and the authority to select the methods to be used in effectuating its goals, as well as to choose the goals themselves. Thus, regardless of its consistency with the basic legislative goal, a private right of action should not be judicially sanctioned if it is incompatible with the enforcement mechanism chosen by the Legislature or with some other aspect of the over-all statutory scheme” (*id.* at 634–635, 543 N.Y.S.2d 18, 541 N.E.2d 18 [citation omitted]; see *Uhr v. East Greenbush Central School Dist.*, 94 N.Y.2d 32, 698 N.Y.S.2d 609, 720 N.E.2d 886 [1999]). *1037 The Court of Appeals, has declined to recognize a private right of action in instances where “[t]he Legislature specifically considered and expressly provided for enforcement mechanisms” in the statute itself (see *Mark G. v. Sabol*, 93 N.Y.2d 710, 720, 695 N.Y.S.2d 730, 717 N.E.2d 1067 [1999]; see also *Cruz v. TD Bank, N.A.*, 22 N.Y.3d 61, 70–71, 979 N.Y.S.2d 257, 2 N.E.3d 221 [2013]).

Although plaintiffs arguably fall within the first two factors, permitting a private right of action for a violation of [General Business Law § 899–aa](#) would not be consistent with Legislature scheme. The enforcement of the statutory provisions has been expressly entrusted to the attorney general. In addition, the Legislature, in subdivision 6(b) stated that “the remedies provided by this section shall be in addition to any other lawful remedy available” and in subdivision 9 stated that “[t]he provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, an locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.” This language, thus, militates against any implied private right of action. In view of the fact that no private right of action exists with respect to [General Business](#)

[Law § 899–aa](#), that branch of the defendants' motion which seeks to dismiss the plaintiffs' first cause of action, is granted.

[10] [11] Plaintiffs second cause of action for negligence per se is based upon [Public Health Law § 18](#). [Public Health Law § 18](#) is designed to ensure, as a general rule, that patients have access to their own medical records (see *Davidson v. State*, 3 A.D.3d 623, 625, 771 N.Y.S.2d 197 [3d Dept.2004]). To the extent that plaintiffs allege that the defendants disclosed their personal and health information to third parties by permitting the theft of the information contained in their data base without plaintiff's consent, this claim fails to state a cause of action. Plaintiffs do not allege that the defendants were participants in the theft of the subject data. Therefore, the theft of the subject data cannot constitute a disclosure of said information. Furthermore, plaintiffs have not established that a private right of action exists with respect to the claimed disclosure of the patients' medical records. Notably, subdivision 12 of this statute provides that “[n]o health care provider shall be subjected to civil liability arising solely from granting or providing access to any patient information in connection with this section”. Therefore *1038 that branch of defendants' motion which seeks to dismiss the second cause of action, is granted.

[12] The third cause of action for negligence per se is based upon [General Business Law § 399–dd \(4\)\(sic\)](#). Plaintiffs' third cause of action is actually based upon [General Business Law § 399–ddd \(4\)](#) which institutes safeguards necessary to thwart unauthorized access to social security numbers. As the enforcement of the provisions of this statute have been entrusted to the attorney general (see [General Business Law § 399–ddd \[7\]](#)), no private **859 right of action exists with respect to a violation of [General Business Law § 399–ddd \(4\)](#). Therefore, that branch of the defendants' motion which seeks to dismiss the third cause of action, is granted.

[13] Plaintiffs' fourth cause of action for negligence per se is based upon HIPPA. As HIPPA and its regulations do not create a private right of action (see *Romanello v. Intesa Sanpaolo S.p.A.*, 97 A.D.3d 449, 455, 949 N.Y.S.2d 345 [1st Dept.2012]; *Jurado v. Kalache*, 29 Misc.3d 1005, 1009, 912 N.Y.S.2d 375 [Sup.Ct., Westchester County 2010]; *Webb v. Smart Document Solutions*, 499 F.3d 1078 [9th Cir.2007]; *Acara v. Banks*, 470 F.3d 569, 571 [5th Cir.2006]; *Cassidy v. Nicolo*, 2005 U.S. Dist. LEXIS 34160, 2005 WL 3334523 [W.D.N.Y.2005]), that branch of the defendants' motion which seeks to dismiss the fourth cause of action, is granted.

[14] Plaintiffs' fifth cause of action for negligence per se is based upon Title XIII, Section 13402, of the American Recovery and Reinvestment Act–Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH, enacted on February 17, 2009, provides for privacy and security of patient health information, and modifies HIPAA by adding new requirements concerning privacy and security for health information. Section 13402, cited in plaintiffs' complaint, is found in 42 U.S.C. § 17921. Although the failure to notify patients of the breach of their Protected Health Information may result in the imposition of penalties by the United States Department of Health and Human Services, neither HITECH nor its governing regulations create a private right of action. Therefore, that branch of the defendants' motion which seeks to dismiss the fifth cause of action, is granted.

The sixth cause of action for a violation of [General Business Law § 349](#) alleges that the defendants “maintained a privacy policy guaranteeing that plaintiffs' protected health information would not be released to any unauthorized third *1039 parties without plaintiffs' consent, and that by “failing to safeguard plaintiffs' protected health information and permitting unauthorized third parties, employees, agents, and/or servants access to plaintiffs' protected health information for illicit and unlawful purposes, in contravention of its privacy policy and other statutory duties detailed above, defendants engaged in a deceptive and unlawful practice.”

[15] [16] [General Business Law § 349](#) provides that “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful” ([General Business Law § 349\[a\]](#)). A private right of action to recover damages for violations of [General Business Law § 349](#) has been provided to “any person who has been injured by reason of any violation of” the statute ([General Business Law § 349\[h\]](#)). Under [General Business Law § 349\(h\)](#), a prima facie case requires a showing that the defendant engaged in a consumer-oriented act or practice that was “deceptive or misleading in a material way and that [the] plaintiff has been injured by reason thereof” ([Goshen v. Mutual Life Ins. Co. of N.Y.](#), 98 N.Y.2d 314, 324, 746 N.Y.S.2d 858, 774 N.E.2d 1190 [2002], quoting [Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank](#), 85 N.Y.2d 20, 25, 623 N.Y.S.2d 529, 647 N.E.2d 741 [1995]). Here, despite the broad language contained in the complaint, the statements allegedly made by defendants in the privacy policy and online notices do not constitute an unlimited guaranty that patient information

could not be stolen or that computerized data could not be hacked. Defendants' alleged failure to safeguard plaintiffs' protected health information and identifying information from **860 theft did not misled the plaintiffs in any material way and does not constitute a deceptive practice within the meaning of the statute (*see Jones v. Bank of Am. N.A.*, 97 A.D.3d 639, 949 N.Y.S.2d 76 [2d Dept.2012]; *see also Ladino v. Bank of Am.*, 52 A.D.3d 571, 574, 861 N.Y.S.2d 683 [2d Dept.2008]). Therefore, that branch of the defendants' motion which seeks to dismiss the sixth cause of action for a violation of [General Business Law § 349](#), is granted.

[17] [18] The seventh cause of action is for breach of contract. The essential elements of a cause of action to recover damages for breach of contract are the existence of a contract, the plaintiff's performance pursuant to the contract, the defendant's breach of its contractual obligations, and damages resulting from the breach (*see El-Nahal v. FA Mgt., Inc.*, 126 A.D.3d 667, 668, 5 N.Y.S.3d 201 [2d Dept.2015]; *Dee v. Rakower*, 112 A.D.3d 204, 208–209, 976 N.Y.S.2d 470 [2d Dept.2013]). In addition, a complaint must “plead the provisions of the contract upon which the cause of action is based.” (*Bello v. *1040 New England Fin.*, 3 Misc.3d 1109(A), 787 N.Y.S.2d 676 [Sup.Ct., Nassau County 2004], citing *Rattenni v. Cerreta*, 285 A.D.2d 636, 728 N.Y.S.2d 401 [2d Dept.2001]; *see also, Sud v. Sud*, 211 A.D.2d 423, 424, 621 N.Y.S.2d 37 [1st Dept.1995]).

[19] Here, plaintiffs allege that they were patients at NSUH, Long Island Jewish Medical Center and other medical facilities, owned or operated by the defendant Health Systems; that the plaintiffs provided personal information to the defendants; that defendants were contractually obligated to the plaintiffs to protect their private health and personal information; and that defendants breached their contractual obligations by “permitting or inadequately protecting against the theft of the Face Sheets containing private health and personal information, and by not acting reasonably to notify and protect plaintiffs and the Class immediately after learning of the thefts and then maliciously failing to notify plaintiffs and the Class in order to knowingly further their own economic interests”. It is alleged that the plaintiffs suffered mentally, physically, financially and emotionally and seek to recover damages, including attorney's fees.

Plaintiffs' allegations are insufficient to state a claim against the defendants for breach of contract. Plaintiffs fail to allege that they each had a contractual relationship with each of the named defendants, and fail to allege any specific provision in

an agreement that the defendants allegedly breached. To the extent that plaintiffs are relying on a privacy statement, either provided to them at the time they received medical services or posted on a website, plaintiffs do not allege that said privacy statement contained any obligation or promise regarding the theft of personal information by third parties. Therefore, that branch of the defendants' motion which seeks to dismiss the seventh cause of action for breach of contract, is granted.

[20] The eighth cause of action is for breach of fiduciary duty. “The elements of a cause of action to recover damages for breach of fiduciary duty are (1) the existence of a fiduciary relationship, (2) misconduct by the defendant, and (3) damages directly caused by the defendant's misconduct” (*Varveris v. Zacharakos*, 110 A.D.3d 1059, 973 N.Y.S.2d 774 [2d Dept.2013]; quoting *Rut v. Young Adult Inst., Inc.*, 74 A.D.3d 776, 777, 901 N.Y.S.2d 715 [2d Dept.2010]; see *1041 *Faith Assembly v. Titledge of N.Y. Abstract, LLC*, 106 A.D.3d 47, 61, 961 N.Y.S.2d 542 [2d Dept.2013]; *Armentano v. Paraco Gas Corp.*, 90 A.D.3d 683, 684, 935 N.Y.S.2d 304 [2d Dept.2011]). A cause of action sounding **861 in breach of fiduciary duty must be pleaded with the particularity required by CPLR 3016(b).

[21] Here, plaintiffs' allegations for breach of fiduciary duty are made collectively against all defendants. Under CPLR 3016(b), a claim for breach of fiduciary must be pleaded with particularity, and the circumstances constituting the alleged wrong must be stated in detail. (see *Palmetto Partners, L.P. v. AJW Qualified Partners, LLC*, 83 A.D.3d 804, 808, 921 N.Y.S.2d 260 [2d Dept.2011]; *Chiu v. Man Choi Chiu*, 71 A.D.3d 621, 623, 896 N.Y.S.2d 132 [2d Dept.2010]). Plaintiffs' group pleading falls far short of this mark. Therefore, that branch of defendants' motion which seeks to dismiss the eighth cause of action for breach of fiduciary duty is granted.

[22] [23] The ninth cause of action is for negligence. “To establish a prima facie case of negligence, a plaintiff must establish the existence of a duty owed by a defendant to the plaintiff, a breach of that duty, and that such breach was the proximate cause of injury to the plaintiff” (*Alvino v. Lin*, 300 A.D.2d 421, 751 N.Y.S.2d 585 [2nd Dept.2002]). Here, plaintiffs allege they gave personal information to the treating facilities in order to receive medical treatment; that these facilities informed the plaintiffs that their personal information would not be disclosed to third parties without their consent; and that an employee or employees of defendants stole their personal information and sold it to third

parties who used said information to open fraudulent credit card accounts, make fraudulent purchases, and fraudulently obtain income tax returns. Plaintiffs allege that they sustained emotional distress, mental anguish, and financial damages as a result of said identity theft. Under these circumstances, the court finds that the ninth cause of action sufficiently states a claim for negligence against defendants Health Systems and NSUH (see *Daly v. Metropolitan Life Insurance Co.*, supra).

With respect to defendants Network and Medical Care, plaintiffs do not allege that they gave any personal or medical information to these entities, and do not specifically allege that these defendants maintained any patient data or were responsible for safeguarding patient data. Plaintiffs' counsel's present assertion that defendants Medical Care, Network, and NSUH are all alter egos of Health Systems, or that they are wholly owned corporate subsidiaries of Health Systems, is not alleged *1042 in the complaint. Therefore, as the complaint does not sufficiently allege any duty owed to the plaintiffs by Medical Care and Network, that branch of the motion which seeks to dismiss the ninth cause of action for negligence is granted as to defendants Network and Medical Care, and is denied as to defendants NSUH and Health Systems.

[24] Plaintiffs, in their tenth cause of action, allege that even if there was no express contractual obligation, defendants owed them a duty of good faith and fair dealing in protecting their personal information from theft. That branch of the defendants' motion which seeks to dismiss the tenth cause of action for breach of the duty of good faith and fair dealing is granted, as such a claim may not be used as a substitute for a nonviable claim of breach of contract (see *StarVest Partners II, L.P. v. Emportal, Inc.*, 101 A.D.3d 610, 957 N.Y.S.2d 93 [1st Dept.2012]; *Sheth v. New York Life Ins. Co.*, 273 A.D.2d 72, 73, 709 N.Y.S.2d 74 [1st Dept.2000]).

[25] In the eleventh cause of action for misrepresentation, plaintiffs allege that the defendants “knowingly, recklessly or negligently failed to timely disclose the material facts to plaintiffs and the Class that their **862 private financial identity, healthy identity and personal information had been stolen, and actively acted to suppress the plaintiffs and the Class from learning of the information thefts, thereby prevented and hindered plaintiffs from taking steps to protect themselves from identity theft or other harm”. Plaintiffs allege that defendants' “misrepresentation by allowing the theft of the Face Sheets and unencrypted computer database and then by not acting reasonably to notify the Class immediately was

deliberate, intentional and wanton.” Plaintiffs allege that they suffered mentally, physically, financially and emotionally.

[26] [27] “The elements of a cause of action sounding in fraud are a material misrepresentation of an existing fact, made with knowledge of the falsity, an intent to induce reliance thereon, justifiable reliance upon the misrepresentation, and damages’ ” (*High Tides, LLC v. DeMichele*, 88 A.D.3d 954, 957, 931 N.Y.S.2d 377[2d Dept.2011] quoting *Introna v. Huntington Learning Ctrs., Inc.*, 78 A.D.3d 896, 898, 911 N.Y.S.2d 442 [2d Dept.2010]; see also *Cremona Food Co., LLC v. Amella*, 130 A.D.3d 559, 12 N.Y.S.3d 293 [2d Dept.2015]). CPLR 3016(b) requires that the circumstances of the fraud must be “stated in detail,” including specific dates and items (see *Moore v. Liberty *1043 Power Corp., LLC*, 72 A.D.3d 660, 661, 897 N.Y.S.2d 723 [2d Dept.2010]). A cause of action to recover damages for fraudulent concealment requires, in addition to allegations of scienter, reliance, and damages, an allegation that the defendant had a duty to disclose material information and that it failed to do so (see *High Tides, LLC v. DeMichele*, 88 A.D.3d at 957, 931 N.Y.S.2d 377; *Manti's Transp., Inc. v. C.T. Lines, Inc.*, 68 A.D.3d 937, 940, 892 N.Y.S.2d 432 [2d Dept.2009]; *Barrett v. Freifeld*, 64 A.D.3d 736, 738, 883 N.Y.S.2d 305 [2d Dept.2009]).

[28] Here, plaintiffs make their fraud allegations collectively as to all defendants. Such group pleading is impermissible.

A fraud claim asserted against multiple defendants must include specific and separate allegations for each defendant (see *Ramos v. Ramirez*, 31 A.D.3d 294, 295, 818 N.Y.S.2d 916 [1st Dept.2006]; see also *Aetna Casualty & Surety Co. v. Merchants Mut. Ins. Co.*, 84 A.D.2d 736, 736, 444 N.Y.S.2d 79 [1st Dept.1981]; *Shareholder Representative Servs. LLC v. Sandoz Inc.*, 46 Misc.3d 1228(A), 2015 WL 1209358 [Sup.Ct., New York County 2015]; *CIFG Assur. N. Am., Inc. v. Bank of America, N.A.*, 41 Misc.3d 1203(A), 2013 WL 5380385 [Sup.Ct., N.Y. County 2013]; *Excel Realty Advisors, L.P. v. SCP Capital, Inc.*, 2010 N.Y. Misc. LEXIS 6067, 2010 WL 5172417 [Sup.Ct., Nassau 2010]). Therefore, defendants' motion to dismiss the eleventh cause of action, is granted.

In view of the foregoing, defendants' motion is granted to the extent that the first, second, third, fourth, fifth, sixth, seventh, eighth, tenth and eleventh causes of action are dismissed in their entirety as to all defendants. That branch of the defendants' motion which seeks to dismiss the ninth cause of action for negligence is granted as to defendants Network and Medical Care, and is denied as to defendants NSUH and Health Systems.

All Citations

49 Misc.3d 1027, 19 N.Y.S.3d 850, 2015 N.Y. Slip Op. 25274

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 to 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.

CHAPTER 266

CRIMINAL LAW AND PROCEDURE

HOUSE BILL 18-1128

BY REPRESENTATIVE(S) Wist and Bridges, Arndt, Becker K., Buckner, Coleman, Danielson, Esgar, Exum, Foote, Garnett, Gray, Hamner, Hansen, Herod, Hooton, Jackson, Kraft-Tharp, Landgraf, Lawrence, Lee, Liston, Lontine, McLachlan, Melton, Michaelson Jenet, Neville P., Pettersen, Rankin, Ransom, Reyher, Roberts, Rosenthal, Saine, Sias, Singer, Valdez, Van Winkle, Weissman, Winkler, Winter, Young, Duran, Benavidez, Ginal, Humphrey, Kennedy, Salazar;
 also SENATOR(S) Lambert and Court, Aguilar, Crowder, Donovan, Fenberg, Fields, Garcia, Gardner, Guzman, Jahn, Jones, Kefalas, Kerr, Lundberg, Marble, Martinez Humenik, Merrifield, Moreno, Neville T., Tate, Todd, Williams A., Zenzinger, Grantham.

AN ACT**CONCERNING STRENGTHENING PROTECTIONS FOR CONSUMER DATA PRIVACY.**

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, 6-1-713, **amend** (1), (2), and (3) as follows:

6-1-713. Disposal of personal identifying information - policy - definitions.

(1) Each ~~public and private~~ COVERED entity in the state that ~~uses~~ MAINTAINS PAPER OR ELECTRONIC documents during the course of business that contain personal identifying information shall develop a WRITTEN policy for the destruction or proper disposal of THOSE paper AND ELECTRONIC documents containing personal identifying information. UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE COVERED ENTITY SHALL DESTROY OR ARRANGE FOR THE DESTRUCTION OF SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR INDECIPHERABLE THROUGH ANY MEANS.

(2) For the purposes of this section AND SECTION 6-1-713.5:

Capital letters or bold & italic numbers indicate new material added to existing statutes; dashes through words indicate deletions from existing statutes and such material not part of act.

(a) "COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION 6-1-102 (6), THAT MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING INFORMATION IN THE COURSE OF THE PERSON'S BUSINESS, VOCATION, OR OCCUPATION. "COVERED ENTITY" DOES NOT INCLUDE A PERSON ACTING AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SECTION 6-1-713.5.

(b) "Personal identifying information" means a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, AS DEFINED IN SECTION 6-1-716 (1)(a); an employer, student, or military identification number; or a financial transaction device, AS DEFINED IN SECTION 18-5-701 (3).

~~(3) A public entity that is managing its records in compliance with part 1 of article 80 of title 24, C.R.S., shall be deemed to have met its obligations under subsection (1) of this section.~~ A COVERED ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR DISPOSAL OF PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

SECTION 2. In Colorado Revised Statutes, **add** 6-1-713.5 as follows:

6-1-713.5. Protection of personal identifying information - definition. (1) TO PROTECT PERSONAL IDENTIFYING INFORMATION, AS DEFINED IN SECTION 6-1-713 (2), FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION, A COVERED ENTITY THAT MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING INFORMATION OF AN INDIVIDUAL RESIDING IN THE STATE SHALL IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE NATURE AND SIZE OF THE BUSINESS AND ITS OPERATIONS.

(2) UNLESS A COVERED ENTITY AGREES TO PROVIDE ITS OWN SECURITY PROTECTION FOR THE INFORMATION IT DISCLOSES TO A THIRD-PARTY SERVICE PROVIDER, THE COVERED ENTITY SHALL REQUIRE THAT THE THIRD-PARTY SERVICE PROVIDER IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE:

(a) APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION DISCLOSED TO THE THIRD-PARTY SERVICE PROVIDER; AND

(b) REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.

(3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE DISCLOSURE OF INFORMATION TO A THIRD PARTY UNDER CIRCUMSTANCES WHERE THE COVERED ENTITY RETAINS PRIMARY RESPONSIBILITY FOR IMPLEMENTING AND MAINTAINING REASONABLE SECURITY PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE COVERED ENTITY

IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS THAT ARE REASONABLY DESIGNED TO:

(a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION; OR

(b) EFFECTIVELY ELIMINATE THE THIRD PARTY'S ABILITY TO ACCESS THE PERSONAL IDENTIFYING INFORMATION, NOTWITHSTANDING THE THIRD PARTY'S PHYSICAL POSSESSION OF THE PERSONAL IDENTIFYING INFORMATION.

(4) A COVERED ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR PROTECTION OF PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

(5) FOR THE PURPOSES OF THIS SECTION, "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED TO MAINTAIN, STORE, OR PROCESS PERSONAL IDENTIFYING INFORMATION ON BEHALF OF A COVERED ENTITY.

SECTION 3. In Colorado Revised Statutes, 6-1-716, **amend** (2), (3), and (4); **repeal and reenact, with amendments**, (1); and **add** (5) as follows:

6-1-716. Notification of security breach. (1) **Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

(b) "COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION 6-1-102 (6), THAT MAINTAINS, OWNS, OR LICENSES PERSONAL INFORMATION IN THE COURSE OF THE PERSON'S BUSINESS, VOCATION, OR OCCUPATION. "COVERED ENTITY" DOES NOT INCLUDE A PERSON ACTING AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SUBSECTION (1)(i) OF THIS SECTION.

(c) "DETERMINATION THAT A SECURITY BREACH OCCURRED" MEANS THE POINT IN TIME AT WHICH THERE IS SUFFICIENT EVIDENCE TO CONCLUDE THAT A SECURITY BREACH HAS TAKEN PLACE.

(d) "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.

(e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY A HEALTH CARE PROFESSIONAL.

(f) "NOTICE" MEANS:

(I) WRITTEN NOTICE TO THE POSTAL ADDRESS LISTED IN THE RECORDS OF THE COVERED ENTITY;

(II) TELEPHONIC NOTICE;

(III) ELECTRONIC NOTICE, IF A PRIMARY MEANS OF COMMUNICATION BY THE COVERED ENTITY WITH A COLORADO RESIDENT IS BY ELECTRONIC MEANS OR THE NOTICE PROVIDED IS CONSISTENT WITH THE PROVISIONS REGARDING ELECTRONIC RECORDS AND SIGNATURES SET FORTH IN THE FEDERAL "ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT", 15 U.S.C. SEC. 7001 ET SEQ.; OR

(IV) SUBSTITUTE NOTICE, IF THE COVERED ENTITY REQUIRED TO PROVIDE NOTICE DEMONSTRATES THAT THE COST OF PROVIDING NOTICE WILL EXCEED TWO HUNDRED FIFTY THOUSAND DOLLARS, THE AFFECTED CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO HUNDRED FIFTY THOUSAND COLORADO RESIDENTS, OR THE COVERED ENTITY DOES NOT HAVE SUFFICIENT CONTACT INFORMATION TO PROVIDE NOTICE. SUBSTITUTE NOTICE CONSISTS OF ALL OF THE FOLLOWING:

(A) E-MAIL NOTICE IF THE COVERED ENTITY HAS E-MAIL ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO RESIDENTS;

(B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE OF THE COVERED ENTITY IF THE COVERED ENTITY MAINTAINS ONE; AND

(C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

(g) (I) (A) "PERSONAL INFORMATION" MEANS A COLORADO RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE: SOCIAL SECURITY NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD NUMBER; MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR BIOMETRIC DATA;

(B) A COLORADO RESIDENT'S USERNAME OR E-MAIL ADDRESS, IN COMBINATION WITH A PASSWORD OR SECURITY QUESTIONS AND ANSWERS, THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

(C) A COLORADO RESIDENT'S ACCOUNT NUMBER OR CREDIT OR DEBIT CARD NUMBER IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO THAT ACCOUNT.

(II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS OR WIDELY DISTRIBUTED MEDIA.

(h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION MAINTAINED BY A COVERED ENTITY. GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN

EMPLOYEE OR AGENT OF A COVERED ENTITY FOR THE COVERED ENTITY'S BUSINESS PURPOSES IS NOT A SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT USED FOR A PURPOSE UNRELATED TO THE LAWFUL OPERATION OF THE BUSINESS OR IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

(i) "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED TO MAINTAIN, STORE, OR PROCESS PERSONAL INFORMATION ON BEHALF OF A COVERED ENTITY.

(2) Disclosure of breach. ~~(a) An individual or a commercial~~ A COVERED entity ~~that conducts business in Colorado and~~ that MAINTAINS, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it ~~becomes aware of a breach of the security of the system~~ BECOMES AWARE THAT A SECURITY BREACH MAY HAVE OCCURRED, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The ~~individual or the commercial~~ COVERED entity shall give notice ~~as soon as possible~~ to the affected Colorado ~~resident~~ RESIDENTS unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice ~~shall~~ MUST be made in the most expedient time possible and without unreasonable delay, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(a.2) IN THE CASE OF A BREACH OF PERSONAL INFORMATION, NOTICE REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO RESIDENTS MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING INFORMATION:

(I) THE DATE, ESTIMATED DATE, OR ESTIMATED DATE RANGE OF THE SECURITY BREACH;

(II) A DESCRIPTION OF THE PERSONAL INFORMATION THAT WAS ACQUIRED OR REASONABLY BELIEVED TO HAVE BEEN ACQUIRED AS PART OF THE SECURITY BREACH;

(III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE COVERED ENTITY TO INQUIRE ABOUT THE SECURITY BREACH;

(IV) THE TOLL-FREE NUMBERS, ADDRESSES, AND WEBSITES FOR CONSUMER REPORTING AGENCIES;

(V) THE TOLL-FREE NUMBER, ADDRESS, AND WEBSITE FOR THE FEDERAL TRADE COMMISSION; AND

(VI) A STATEMENT THAT THE RESIDENT CAN OBTAIN INFORMATION FROM THE FEDERAL TRADE COMMISSION AND THE CREDIT REPORTING AGENCIES ABOUT FRAUD ALERTS AND SECURITY FREEZES.

(a.3) IF AN INVESTIGATION BY THE COVERED ENTITY PURSUANT TO SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE TYPE OF PERSONAL INFORMATION

DESCRIBED IN SUBSECTION (1)(g)(I)(B) OF THIS SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE MISUSED, THEN THE COVERED ENTITY SHALL, IN ADDITION TO THE NOTICE OTHERWISE REQUIRED BY SUBSECTION (2)(a.2) OF THIS SECTION AND IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM:

(I) DIRECT THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED TO PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE COVERED ENTITY AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED USES THE SAME USERNAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR ANSWER.

(II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED BY THE COVERED ENTITY, THE COVERED ENTITY SHALL NOT COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT E-MAIL ADDRESS, BUT MAY INSTEAD COMPLY WITH THIS SECTION BY PROVIDING NOTICE THROUGH OTHER METHODS, AS DEFINED IN SUBSECTION (1)(f) OF THIS SECTION, 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 COVERED ENTITY KNOWS THE RESIDENT CUSTOMARILY ACCESSES THE ACCOUNT.

(a.4) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED.

(a.5) A COVERED ENTITY THAT IS REQUIRED TO PROVIDE NOTICE TO AFFECTED COLORADO RESIDENTS PURSUANT TO THIS SUBSECTION (2) IS PROHIBITED FROM CHARGING THE COST OF PROVIDING SUCH NOTICE TO SUCH RESIDENTS.

(a.6) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY STATE OR FEDERAL LAW.

(b) ~~An individual or a commercial entity that maintains~~ IF A COVERED ENTITY USES A THIRD-PARTY SERVICE PROVIDER TO MAINTAIN computerized data that includes personal information, ~~that the individual or the commercial entity does not own or license~~ THEN THE THIRD-PARTY SERVICE PROVIDER shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately THE COVERED ENTITY IN THE EVENT OF A SECURITY BREACH THAT COMPROMISES SUCH COMPUTERIZED DATA, INCLUDING NOTIFYING THE COVERED ENTITY OF ANY SECURITY BREACH IN THE MOST EXPEDIENT TIME POSSIBLE, AND WITHOUT UNREASONABLE DELAY following discovery of a SECURITY breach,

if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the ~~owner or licensee~~ COVERED ENTITY information relevant to the SECURITY breach; except that such cooperation ~~shall not be deemed to~~ DOES NOT require the disclosure of confidential business information or trade secrets.

(c) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the ~~individual or commercial~~ COVERED entity that conducts business in Colorado not to send notice required by this section. Notice required by this section ~~shall~~ MUST be made in good faith, IN THE MOST EXPEDIENT TIME POSSIBLE AND without unreasonable delay ~~and as soon as possible~~ BUT NOT LATER THAN THIRTY DAYS after the law enforcement agency determines that notification will no longer impede the investigation and has notified the ~~individual or commercial~~ COVERED entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

(d) If ~~an individual or commercial~~ A COVERED entity is required to notify more than one thousand Colorado residents of a SECURITY breach ~~of the security of the system~~ pursuant to this section, the ~~individual or commercial~~ COVERED entity shall also notify, IN THE MOST EXPEDIENT TIME POSSIBLE AND without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by THE FEDERAL "FAIR CREDIT REPORTING ACT", 15 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this ~~paragraph (d) shall be construed to require~~ SUBSECTION (2)(d) REQUIRES the ~~individual or commercial~~ COVERED entity to provide to the consumer reporting agency the names or other personal information of SECURITY breach notice recipients. This ~~paragraph (d) shall~~ SUBSECTION (2)(d) DOES not apply to a ~~person~~ COVERED ENTITY who is subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

(e) A WAIVER OF THESE NOTIFICATION RIGHTS OR RESPONSIBILITIES IS VOID AS AGAINST PUBLIC POLICY.

(f) (I) THE COVERED ENTITY THAT MUST NOTIFY COLORADO RESIDENTS OF A DATA BREACH PURSUANT TO THIS SECTION SHALL PROVIDE NOTICE OF ANY SECURITY BREACH TO THE COLORADO ATTORNEY GENERAL IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, IF THE SECURITY BREACH IS REASONABLY BELIEVED TO HAVE AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR MORE, UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS NOT LIKELY TO OCCUR.

(II) THE COLORADO ATTORNEY GENERAL SHALL DESIGNATE A PERSON OR PERSONS AS A POINT OF CONTACT FOR FUNCTIONS SET FORTH IN THIS SUBSECTION (2)(f) AND SHALL MAKE THE CONTACT INFORMATION FOR THAT PERSON OR THOSE PERSONS PUBLIC ON THE ATTORNEY GENERAL'S WEBSITE AND BY ANY OTHER APPROPRIATE MEANS.

(g) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED IN THE SECURITY BREACH.

(3) Procedures deemed in compliance with notice requirements. (a) ~~Under~~ PURSUANT TO this section, ~~an individual or a commercial~~ A COVERED entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section ~~shall be deemed to be~~ is in compliance with the notice requirements of this section if the ~~individual or the commercial~~ COVERED entity notifies affected Colorado ~~customers~~ RESIDENTS in accordance with its policies in the event of a ~~breach of security of the system~~ SECURITY BREACH; EXCEPT THAT NOTICE TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(f) OF THIS SECTION.

(b) ~~An individual or a commercial~~ A COVERED entity that is regulated by state or federal law and that maintains procedures for a SECURITY breach ~~of the security of the system~~ pursuant to the laws, rules, regulations, guidances, or guidelines established by its ~~primary or functional~~ state or federal regulator is ~~deemed to be~~ in compliance with this section; EXCEPT THAT NOTICE TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(f) OF THIS SECTION. IN THE CASE OF A CONFLICT BETWEEN THE TIME PERIOD FOR NOTICE TO INDIVIDUALS THAT IS REQUIRED PURSUANT TO THIS SUBSECTION (3) AND THE APPLICABLE STATE OR FEDERAL LAW OR REGULATION, THE LAW OR REGULATION WITH THE SHORTEST TIME FRAME FOR NOTICE TO THE INDIVIDUAL CONTROLS.

(4) Violations. The attorney general may bring an action in law or equity to address violations of this section, SECTION 6-1-713, OR SECTION 6-1-713.5, and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve ~~an individual or a commercial~~ A COVERED entity subject to this section from compliance with all other applicable provisions of law.

(5) Attorney general criminal authority. UPON RECEIPT OF NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, AND WITH EITHER A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE COULD BE BROUGHT, THE ATTORNEY GENERAL HAS THE AUTHORITY TO PROSECUTE ANY CRIMINAL VIOLATIONS OF SECTION 18-5.5-102.

SECTION 4. In Colorado Revised Statutes, **add** article 73 to title 24 as follows:

ARTICLE 73
Security Breaches and Personal Information

24-73-101. Governmental entity - disposal of personal identifying information - policy - definitions. (1) ~~EACH~~ GOVERNMENTAL ENTITY IN THE STATE THAT MAINTAINS PAPER OR ELECTRONIC DOCUMENTS DURING THE COURSE OF

BUSINESS THAT CONTAIN PERSONAL IDENTIFYING INFORMATION SHALL DEVELOP A WRITTEN POLICY FOR THE DESTRUCTION OR PROPER DISPOSAL OF THOSE PAPER AND ELECTRONIC DOCUMENTS CONTAINING PERSONAL IDENTIFYING INFORMATION. UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE GOVERNMENTAL ENTITY DESTROY OR ARRANGE FOR THE DESTRUCTION OF SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR INDECIPHERABLE THROUGH ANY MEANS.

(2) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR DISPOSAL OF PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

(3) UNLESS A GOVERNMENTAL ENTITY SPECIFICALLY CONTRACTS WITH A RECYCLER OR DISPOSAL FIRM FOR DESTRUCTION OF DOCUMENTS THAT CONTAIN PERSONAL IDENTIFYING INFORMATION, NOTHING IN THIS SECTION REQUIRES A RECYCLER OR DISPOSAL FIRM TO VERIFY THAT THE DOCUMENTS CONTAINED IN THE PRODUCTS IT RECEIVES FOR DISPOSAL OR RECYCLING HAVE BEEN PROPERLY DESTROYED OR DISPOSED OF AS REQUIRED BY THIS SECTION.

(4) FOR THE PURPOSES OF THIS SECTION AND SECTION 24-73-102, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(a) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE AGENCY OR INSTITUTION, INCLUDING THE JUDICIAL DEPARTMENT, COUNTY, CITY AND COUNTY, INCORPORATED CITY OR TOWN, SCHOOL DISTRICT, SPECIAL IMPROVEMENT DISTRICT, AUTHORITY, AND EVERY OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR POLITICAL SUBDIVISION OF THE STATE ORGANIZED PURSUANT TO LAW. "GOVERNMENTAL ENTITY" INCLUDES ENTITIES GOVERNED BY HOME RULE CHARTERS. "GOVERNMENTAL ENTITY" DOES NOT INCLUDE AN ENTITY ACTING AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SECTION 24-73-102.

(b) "PERSONAL IDENTIFYING INFORMATION" MEANS A SOCIAL SECURITY NUMBER; A PERSONAL IDENTIFICATION NUMBER; A PASSWORD; A PASS CODE; AN OFFICIAL STATE OR GOVERNMENT-ISSUED DRIVER'S LICENSE OR IDENTIFICATION CARD NUMBER; A GOVERNMENT PASSPORT NUMBER; BIOMETRIC DATA, AS DEFINED IN SECTION 24-73-103 (1)(a); AN EMPLOYER, STUDENT, OR MILITARY IDENTIFICATION NUMBER; OR A FINANCIAL TRANSACTION DEVICE, AS DEFINED IN SECTION 18-5-701 (3).

24-73-102. Governmental entity - protection of personal identifying information - definition. (1) TO PROTECT PERSONAL IDENTIFYING INFORMATION, AS DEFINED IN SECTION 24-73-101 (4)(b), FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION, A GOVERNMENTAL ENTITY THAT MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING INFORMATION SHALL

IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE NATURE AND SIZE OF THE GOVERNMENTAL ENTITY.

(2) UNLESS A GOVERNMENTAL ENTITY AGREES TO PROVIDE ITS OWN SECURITY PROTECTION FOR THE INFORMATION IT DISCLOSES TO A THIRD-PARTY SERVICE PROVIDER, THE GOVERNMENTAL ENTITY SHALL REQUIRE THAT THE THIRD-PARTY SERVICE PROVIDER IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE:

(a) APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION DISCLOSED TO THE THIRD-PARTY SERVICE PROVIDER; AND

(b) REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.

(3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE DISCLOSURE OF INFORMATION TO A THIRD PARTY UNDER CIRCUMSTANCES WHERE THE GOVERNMENTAL ENTITY RETAINS PRIMARY RESPONSIBILITY FOR IMPLEMENTING AND MAINTAINING REASONABLE SECURITY PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE GOVERNMENTAL ENTITY IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS REASONABLY DESIGNED TO:

(a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, MODIFICATION, DISCLOSURE, OR DESTRUCTION; OR

(b) EFFECTIVELY ELIMINATE THE THIRD PARTY'S ABILITY TO ACCESS THE PERSONAL IDENTIFYING INFORMATION, NOTWITHSTANDING THE THIRD PARTY'S PHYSICAL POSSESSION OF THE PERSONAL IDENTIFYING INFORMATION.

(4) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR STORAGE OF PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

(5) FOR THE PURPOSES OF THIS SECTION, "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED TO MAINTAIN, STORE, OR PROCESS PERSONAL IDENTIFYING INFORMATION ON BEHALF OF A GOVERNMENTAL ENTITY.

24-73-103. Governmental entity - notification of security breach.

(1) **Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

(b) "DETERMINATION THAT A SECURITY BREACH OCCURRED" MEANS THE POINT IN TIME AT WHICH THERE IS SUFFICIENT EVIDENCE TO CONCLUDE THAT A SECURITY BREACH HAS TAKEN PLACE.

(c) "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.

(d) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE AGENCY OR INSTITUTION, INCLUDING THE JUDICIAL DEPARTMENT, COUNTY, CITY AND COUNTY, INCORPORATED CITY OR TOWN, SCHOOL DISTRICT, SPECIAL IMPROVEMENT DISTRICT, AUTHORITY, AND EVERY OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR POLITICAL SUBDIVISION OF THE STATE ORGANIZED PURSUANT TO LAW. "GOVERNMENTAL ENTITY" INCLUDES ENTITIES GOVERNED BY HOME RULE CHARTERS. "GOVERNMENTAL ENTITY" DOES NOT INCLUDE AN ENTITY ACTING AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SUBSECTION (1)(i) OF THIS SECTION.

(e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY A HEALTH CARE PROFESSIONAL.

(f) "NOTICE" MEANS:

(I) WRITTEN NOTICE TO THE POSTAL ADDRESS LISTED IN THE RECORDS OF THE GOVERNMENTAL ENTITY;

(II) TELEPHONIC NOTICE;

(III) ELECTRONIC NOTICE, IF A PRIMARY MEANS OF COMMUNICATION BY THE GOVERNMENTAL ENTITY WITH A COLORADO RESIDENT IS BY ELECTRONIC MEANS OR THE NOTICE PROVIDED IS CONSISTENT WITH THE PROVISIONS REGARDING ELECTRONIC RECORDS AND SIGNATURES SET FORTH IN THE FEDERAL "ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT", 15 U.S.C. SEC. 7001 ET SEQ.; OR

(IV) SUBSTITUTE NOTICE, IF THE GOVERNMENTAL ENTITY REQUIRED TO PROVIDE NOTICE DEMONSTRATES THAT THE COST OF PROVIDING NOTICE WILL EXCEED TWO HUNDRED FIFTY THOUSAND DOLLARS, THE AFFECTED CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO HUNDRED FIFTY THOUSAND COLORADO RESIDENTS, OR THE GOVERNMENTAL ENTITY DOES NOT HAVE SUFFICIENT CONTACT INFORMATION TO PROVIDE NOTICE. SUBSTITUTE NOTICE CONSISTS OF ALL OF THE FOLLOWING:

(A) E-MAIL NOTICE IF THE GOVERNMENTAL ENTITY HAS E-MAIL ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO RESIDENTS;

(B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE OF THE GOVERNMENTAL ENTITY IF THE GOVERNMENTAL ENTITY MAINTAINS ONE; AND

(C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

(g) (I) (A) "PERSONAL INFORMATION" MEANS A COLORADO RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE: SOCIAL SECURITY NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION NUMBER; MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR BIOMETRIC DATA, AS DEFINED IN SUBSECTION (1)(a) OF THIS SECTION;

(B) A COLORADO RESIDENT'S USERNAME OR E-MAIL ADDRESS, IN COMBINATION WITH A PASSWORD OR SECURITY QUESTIONS AND ANSWERS, THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

(C) A COLORADO RESIDENT'S ACCOUNT NUMBER OR CREDIT OR DEBIT CARD NUMBER IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO THAT ACCOUNT.

(II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS OR WIDELY DISTRIBUTED MEDIA.

(h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION MAINTAINED BY A GOVERNMENTAL ENTITY. GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A GOVERNMENTAL ENTITY FOR THE PURPOSES OF THE GOVERNMENTAL ENTITY IS NOT A SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT USED FOR A PURPOSE UNRELATED TO THE LAWFUL GOVERNMENT PURPOSE OR IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

(i) "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED TO MAINTAIN, STORE, OR PROCESS PERSONAL INFORMATION ON BEHALF OF A GOVERNMENTAL ENTITY.

(2) **Disclosure of breach.** (a) A GOVERNMENTAL ENTITY THAT MAINTAINS, OWNS, OR LICENSES COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION ABOUT A RESIDENT OF COLORADO SHALL, WHEN IT BECOMES AWARE THAT A SECURITY BREACH MAY HAVE OCCURRED, CONDUCT IN GOOD FAITH A PROMPT INVESTIGATION TO DETERMINE THE LIKELIHOOD THAT PERSONAL INFORMATION HAS BEEN OR WILL BE MISUSED. THE GOVERNMENTAL ENTITY SHALL GIVE NOTICE TO THE AFFECTED COLORADO RESIDENTS UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS NOT REASONABLY LIKELY TO OCCUR. NOTICE MUST BE MADE IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM.

(b) IN THE CASE OF A BREACH OF PERSONAL INFORMATION, NOTICE REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO RESIDENTS MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING INFORMATION:

(I) THE DATE, ESTIMATED DATE, OR ESTIMATED DATE RANGE OF THE SECURITY BREACH;

(II) A DESCRIPTION OF THE PERSONAL INFORMATION THAT WAS ACQUIRED OR REASONABLY BELIEVED TO HAVE BEEN ACQUIRED AS PART OF THE SECURITY BREACH;

(III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE GOVERNMENTAL ENTITY TO INQUIRE ABOUT THE SECURITY BREACH;

(IV) THE TOLL-FREE NUMBERS, ADDRESSES, AND WEBSITES FOR CONSUMER REPORTING AGENCIES;

(V) THE TOLL-FREE NUMBER, ADDRESS, AND WEBSITE FOR THE FEDERAL TRADE COMMISSION; AND

(VI) A STATEMENT THAT THE RESIDENT CAN OBTAIN INFORMATION FROM THE FEDERAL TRADE COMMISSION AND THE CREDIT REPORTING AGENCIES ABOUT FRAUD ALERTS AND SECURITY FREEZES.

(c) IF AN INVESTIGATION BY THE GOVERNMENTAL ENTITY PURSUANT TO SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE TYPE OF PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B) OF THIS SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE MISUSED, THEN THE GOVERNMENTAL ENTITY SHALL, IN ADDITION TO THE NOTICE OTHERWISE REQUIRED BY SUBSECTION (2)(b) OF THIS SECTION AND IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM:

(I) DIRECT THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED TO PROMPTLY CHANGE HIS OR HER 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 E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR ANSWER.

(II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED BY THE GOVERNMENTAL ENTITY, THE GOVERNMENTAL ENTITY SHALL NOT COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT E-MAIL ADDRESS, BUT MAY INSTEAD COMPLY WITH THIS SECTION BY PROVIDING NOTICE THROUGH OTHER METHODS, AS DEFINED IN SUBSECTION (1)(f) OF THIS SECTION, 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 GOVERNMENTAL ENTITY KNOWS THE RESIDENT CUSTOMARILY ACCESSES THE ACCOUNT.

(d) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED.

(e) A GOVERNMENTAL ENTITY THAT IS REQUIRED TO PROVIDE NOTICE PURSUANT TO THIS SUBSECTION (2) IS PROHIBITED FROM CHARGING THE COST OF PROVIDING SUCH NOTICE TO INDIVIDUALS.

(f) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY STATE OR FEDERAL LAW.

(g) IF A GOVERNMENTAL ENTITY USES A THIRD-PARTY SERVICE PROVIDER TO MAINTAIN COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION, THEN THE THIRD-PARTY SERVICE PROVIDER SHALL GIVE NOTICE TO AND COOPERATE WITH THE GOVERNMENTAL ENTITY IN THE EVENT OF A SECURITY BREACH THAT COMPROMISES SUCH COMPUTERIZED DATA, INCLUDING NOTIFYING THE GOVERNMENTAL ENTITY OF ANY SECURITY BREACH IN THE MOST EXPEDIENT TIME AND WITHOUT UNREASONABLE DELAY FOLLOWING DISCOVERY OF A SECURITY BREACH, IF MISUSE OF PERSONAL INFORMATION ABOUT A COLORADO RESIDENT OCCURRED OR IS LIKELY TO OCCUR. COOPERATION INCLUDES SHARING WITH THE COVERED ENTITY INFORMATION RELEVANT TO THE SECURITY BREACH; EXCEPT THAT SUCH COOPERATION DOES NOT REQUIRE THE DISCLOSURE OF CONFIDENTIAL BUSINESS INFORMATION OR TRADE SECRETS.

(h) NOTICE REQUIRED BY THIS SECTION MAY BE DELAYED IF A LAW ENFORCEMENT AGENCY DETERMINES THAT THE NOTICE WILL IMPEDE A CRIMINAL INVESTIGATION AND THE LAW ENFORCEMENT AGENCY HAS NOTIFIED THE GOVERNMENTAL ENTITY THAT OPERATES IN COLORADO NOT TO SEND NOTICE REQUIRED BY THIS SECTION. NOTICE REQUIRED BY THIS SECTION MUST BE MADE IN GOOD FAITH, IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE LAW ENFORCEMENT AGENCY DETERMINES THAT NOTIFICATION WILL NO LONGER IMPEDE THE INVESTIGATION, AND HAS NOTIFIED THE GOVERNMENTAL ENTITY THAT IT IS APPROPRIATE TO SEND THE NOTICE REQUIRED BY THIS SECTION.

(i) IF A GOVERNMENTAL ENTITY IS REQUIRED TO NOTIFY MORE THAN ONE THOUSAND COLORADO RESIDENTS OF A SECURITY BREACH PURSUANT TO THIS SECTION, THE GOVERNMENTAL ENTITY SHALL ALSO NOTIFY, IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, ALL CONSUMER REPORTING AGENCIES THAT COMPILE AND MAINTAIN FILES ON CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED BY THE FEDERAL "FAIR CREDIT REPORTING ACT", 15 U.S.C. SEC. 1681a (p), OF THE ANTICIPATED DATE OF THE NOTIFICATION TO THE RESIDENTS AND THE APPROXIMATE NUMBER OF RESIDENTS WHO ARE TO BE NOTIFIED. NOTHING IN THIS SUBSECTION (2)(i) REQUIRES THE GOVERNMENTAL ENTITY TO PROVIDE TO THE CONSUMER REPORTING AGENCY THE NAMES OR OTHER PERSONAL INFORMATION OF

SECURITY BREACH NOTICE RECIPIENTS. THIS SUBSECTION (2)(i) DOES NOT APPLY TO A PERSON WHO IS SUBJECT TO TITLE V OF THE FEDERAL "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ.

(j) A WAIVER OF THESE NOTIFICATION RIGHTS OR RESPONSIBILITIES IS VOID AS AGAINST PUBLIC POLICY.

(k) (I) THE GOVERNMENTAL ENTITY THAT MUST NOTIFY COLORADO RESIDENTS OF A DATA BREACH PURSUANT TO THIS SECTION SHALL PROVIDE NOTICE OF ANY SECURITY BREACH TO THE COLORADO ATTORNEY GENERAL IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, IF THE SECURITY BREACH IS REASONABLY BELIEVED TO HAVE AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR MORE, UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS NOT LIKELY TO OCCUR.

(II) THE COLORADO ATTORNEY GENERAL SHALL DESIGNATE A PERSON OR PERSONS AS A POINT OF CONTACT FOR FUNCTIONS SET FORTH IN THIS SUBSECTION (2)(k) AND SHALL MAKE THE CONTACT INFORMATION FOR THAT PERSON OR THOSE PERSONS PUBLIC ON THE ATTORNEY GENERAL'S WEBSITE AND BY ANY OTHER APPROPRIATE MEANS.

(l) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED IN THE SECURITY BREACH.

(3) Procedures deemed in compliance with notice requirements.

(a) PURSUANT TO THIS SECTION, A GOVERNMENTAL ENTITY THAT MAINTAINS ITS OWN NOTIFICATION PROCEDURES AS PART OF AN INFORMATION SECURITY POLICY FOR THE TREATMENT OF PERSONAL INFORMATION AND WHOSE PROCEDURES ARE OTHERWISE CONSISTENT WITH THE TIMING REQUIREMENTS OF THIS SECTION IS IN COMPLIANCE WITH THE NOTICE REQUIREMENTS OF THIS SECTION IF THE GOVERNMENTAL ENTITY NOTIFIES AFFECTED COLORADO RESIDENTS IN ACCORDANCE WITH ITS POLICIES IN THE EVENT OF A SECURITY BREACH; EXCEPT THAT NOTICE TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(k) OF THIS SECTION.

(b) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR A SECURITY BREACH PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION; EXCEPT THAT NOTICE TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(k) OF THIS SECTION. IN THE CASE OF A CONFLICT BETWEEN THE TIME PERIOD FOR NOTICE TO INDIVIDUALS, THE LAW OR REGULATION WITH THE SHORTEST NOTICE PERIOD CONTROLS.

(4) Violations. THE ATTORNEY GENERAL MAY BRING AN ACTION FOR INJUNCTIVE RELIEF TO ENFORCE THE PROVISIONS OF THIS SECTION.

(5) **Attorney general criminal authority.** UPON RECEIPT OF NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, AND WITH EITHER A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE COULD BE BROUGHT, THE ATTORNEY GENERAL HAS THE AUTHORITY TO PROSECUTE ANY CRIMINAL VIOLATIONS OF SECTION 18-5.5-102.

SECTION 5. Effective date. This act takes effect September 1, 2018.

SECTION 6. Safety clause. The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

Approved: May 29, 2018

Article 3

EU GDPR

"Territorial scope"

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to 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 behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.



KeyCite Yellow Flag - Negative Treatment

Distinguished by [Prime Foods for Processing and Trading v. Greater Omaha Packing Co., Inc.](#), D.Neb., June 4, 2019

362 F.Supp.3d 1295
United States District Court,
N.D. Georgia, Atlanta Division.

IN RE EQUIFAX, INC., CUSTOMER
DATA SECURITY BREACH LITIGATION

MDL DOCKET NO. 2800

|
1:17-md-2800-TWT

|
Signed January 28, 2019

Synopsis

Background: Consumers brought putative class action against consumer reporting agency and affiliated entities, alleging various claims, including violation of the Fair Credit Reporting Act (FCRA) and negligence under Georgia law, arising from data breach in which personal and financial information of nearly 150 million Americans was potentially stolen. Defendants moved to dismiss.

Holdings: The District Court, [Thomas W. Thrash, Jr.](#), J., held that:

[1] under Georgia choice of law rules, district court would apply Georgia law;

[2] consumers failed to state claim under the FCRA;

[3] consumers stated negligence claim under Georgia law;

[4] consumers stated negligence per se claim under Georgia law;

[5] consumers failed to state breach of contract claim under Georgia law;

[6] consumers stated claims for violation of various state fraud and consumer protection statutes; and

[7] consumers adequately alleged claims for violation of various state data-breach statutes.

Motion granted in part and denied in part.

West Headnotes (87)

[1] **Federal Civil Procedure**

🔑 **Insufficiency in general**

A complaint may survive a motion to dismiss for failure to state a claim even if it is improbable that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely remote and unlikely. [Fed. R. Civ. P. 12\(b\)\(6\)](#).

[2] **Federal Civil Procedure**

🔑 **Claim for relief in general**

Generally, notice pleading is all that is required for a valid complaint. [Fed. R. Civ. P. 8](#).

[3] **Federal Civil Procedure**

🔑 **Claim for relief in general**

Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests. [Fed. R. Civ. P. 8](#).

[4] **Torts**

🔑 **What law governs**

Georgia's choice of law rules follows the traditional approach of *lex loci delicti* in tort cases, which generally applies the substantive law of the state where the last event occurred necessary to make an actor liable for the alleged tort; usually, this means that the law of the place of the injury governs rather than the law of the place of the tortious acts allegedly causing the injury.

[5] **Action**

🔑 **What law governs**

Under Georgia choice of law rules, application of another jurisdiction's laws is limited to statutes

and decisions construing those statutes; when no statute is involved, Georgia courts apply the common law as developed in Georgia rather than foreign case law.

[6] **Negligence**

🔑 [What law governs](#)

Under Georgia choice of law rules, district court, in putative class action, would apply Georgia law to action brought by consumers, who were located in various states, against consumer reporting agency and affiliated agencies located in Georgia, alleging, inter alia, negligence under Georgia law, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, even though the alleged injuries occurred in various jurisdictions; consumers identified no foreign statutes that governed their common law claims.

[7] **Finance, Banking, and Credit**

🔑 [Reports subject to regulation](#)

Finance, Banking, and Credit

🔑 [Identity theft in general](#)

Consumers, in putative class action, failed to allege that consumer reporting agency furnished consumer reports to cyberhackers, as required to state claim under the Fair Credit Reporting Act (FCRA) against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, even if agency's conduct was egregious; the data at issue was stolen by cyberhackers and not furnished to them. Consumer Credit Protection Act § 604, [15 U.S.C.A. § 1681b\(a\)](#).

[8] **Finance, Banking, and Credit**

🔑 [Reports subject to regulation](#)

Finance, Banking, and Credit

🔑 [Identity theft in general](#)

Personally identifying information stolen in data breach was not a consumer report within meaning of Fair Credit Reporting Act

(FCRA), as required for consumers, in putative class action, to state claim under the FCRA against consumer reporting agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; cyberhackers did not obtain access to the active credit files maintained by agency, cyberhackers only obtained legacy data, such data did not bear on an individual's credit worthiness, and information in data, including Social Security numbers and dates of birth, did not, by itself, constitute a credit report. Consumer Credit Protection Act § 604, [15 U.S.C.A. § 1681b](#).

[1 Cases that cite this headnote](#)

[9] **Finance, Banking, and Credit**

🔑 [Obligations of Reporting Agencies](#)

A plaintiff bringing a claim that a consumer reporting agency violated the reasonable procedures requirement of provision of the Fair Credit Reporting Act (FCRA) governing compliance procedures must first show that the reporting agency released the report in violation of FCRA provision governing permissible purposes of consumer reports. Consumer Credit Protection Act §§ 604, 607, [15 U.S.C.A. §§ 1681b, 1681e](#).

[10] **Finance, Banking, and Credit**

🔑 [Disclosures to consumer](#)

Finance, Banking, and Credit

🔑 [Identity theft in general](#)

Consumers, in putative class action, failed to state claim against credit reporting agency and affiliated entities under Fair Credit Report Act (FCRA) provision governing disclosures to consumers, based on agency allegedly failing, upon request, to disclose to consumers all of the information in their consumer files by failing to identify data breach and the cyberhackers who procured consumers' information, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; cyberhackers did not obtain a consumer report within meaning of the FCRA,

and agency could not have been expected to disclose identity of unknown cyberhackers. Consumer Credit Protection Act §§ 604, 609, 15 U.S.C.A. §§ 1681b, 1681g(a).

[11] Negligence

🔑 Elements in general

Under Georgia law, before an action for a tort will lie, the plaintiff must show he sustained injury or damage as a result of the negligent act or omission to act in some duty owed to him.

[12] Torts

🔑 Injury or Damage from Act

Although, under Georgia law, nominal damages can be awarded where there has been an injury but the injury is small, where there is no evidence of injury accompanying the tort, an essential element of the tort is lacking, thereby entitling the defendant to judgment in his favor.

[13] Finance, Banking, and Credit

🔑 Identity theft in general

Consumers, in putative class action, adequately alleged that compromise of personally identifiable information constituted actual cognizable injury, as required to state tort claims against consumer reporting agency and affiliated entities under Georgia law for, inter alia, negligence and negligence per se, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, despite contention that fear of future damages from identity theft was too speculative; consumers alleged that they were harmed by having to take measures to combat identity theft risk, that identity theft already occurred to some consumers, and that all consumers faced serious and imminent risk of fraud and identity theft due to vast amount of information stolen.

[1 Cases that cite this headnote](#)

[14] Negligence

🔑 Violations of statutes and other regulations

Consumers, in putative class action, adequately alleged that unauthorized charges on their payment cards, which purportedly was result of consumer reporting agency's data breach, were actual, concrete injuries that were legally cognizable, as required to state tort claims based on the payment card fraud against agency and affiliated entities under Georgia law, for, inter alia, negligence and negligence per se, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, even though agency argued that consumers were required to allege dates that charges were made and that they were not reimbursed for charges; consumers' allegations that such charges occurred was sufficient.

[15] Negligence

🔑 Necessity of legal or proximate causation

Before any negligence, even if proven, can be actionable under Georgia law, that negligence must be the proximate cause of the injuries sued upon.

[16] Negligence

🔑 Requisites, Definitions and Distinctions

To establish proximate cause, as required to support negligence claim under Georgia law, a plaintiff must show a legally attributable causal connection between the defendant's conduct and the alleged injury.

[17] Negligence

🔑 In general; degrees of proof

In order to establish proximate cause, as required to state a negligence claim under Georgia law, a plaintiff must establish that it is more likely than not that the conduct of the defendant was a cause in fact of the result.

[18] Negligence

🔑 In general; degrees of proof

A mere possibility of proximate causation is not enough, in order to establish the proximate cause required to support a negligence claim under Georgia law.

[19] Federal Civil Procedure

🔑 Tort cases in general

When the matter of whether there is proximate cause, as required to support negligence claim under Georgia law, remains one of pure speculation or conjecture, or the probabilities are at best evenly balanced, it becomes the duty of the court to grant summary judgment for the defendant.

[20] Finance, Banking, and Credit

🔑 Identity theft in general

Consumers, in putative class action, adequately alleged proximate cause based on injuries, including identity theft, resulting specifically from consumer reporting agency's data breach, as required to state tort claims for, inter alia, negligence under Georgia law, against consumer reporting agency and related entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged that agency had custody of their personally identifiable information, that agency's systems were hacked, that these cyberhackers obtained that information, and that as a result of breach consumers became victims of identity theft and other fraudulent activity, and that many consumers purchased credit monitoring and incurred other costs in direct response to agency's data breach.

[1 Cases that cite this headnote](#)

[21] Negligence

🔑 Protection against acts of third persons

Generally, under Georgia law, there is no duty to prevent the unforeseeable intervening criminal act of a third person.

[22] Negligence

🔑 In general; foreseeability of other cause

Under Georgia law, when a defendant claims that its negligence is not the proximate cause of the plaintiff's injuries, but that an act of a third party intervened to cause those injuries, the rule is that an intervening and independent wrongful act of a third person producing the injury, and without which it would not have occurred, should be treated as the proximate cause, insulating and excluding the negligence of the defendant.

[23] Negligence

🔑 In general; foreseeability of other cause

The rule, under Georgia law, that the intervening and independent wrongful act of a third person producing the plaintiff's injury, and without which it would not have occurred, should be treated as the proximate cause, insulating and excluding the negligence of the defendant, does not insulate the defendant if the defendant had reasonable grounds for apprehending that such wrongful act would be committed.

[24] Negligence

🔑 In general; foreseeability of other cause

Under Georgia law, if the character of the intervening act by a third-party claimed to break the connection between the defendant's original wrongful act and the subsequent injury was such that its probable or natural consequences could reasonably have been anticipated, apprehended, or foreseen by the original wrong-doer, the causal connection is not broken, and the original wrong-doer is responsible for all of the consequences resulting from the intervening act.

[25] Negligence

🔑 Protection against acts of third persons

Under Georgia law, question of reasonable foreseeability of a third-party's criminal attack, as could prevent a defendant from being insulated from liability for the attack, is generally for a jury to determine.

[26] Finance, Banking, and Credit**🔑 Identity theft in general**

Consumers, in putative class action, sufficiently alleged that criminal actions of third-party cyberhackers responsible for data breach were reasonably foreseeable, and thus did not insulate consumer reporting agency and related entities from liability for purposes of consumers' tort claims in putative class action for, inter alia, negligence and negligence per se under Georgia law, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged that agency observed major data breaches at other corporations, that agency itself experienced prior data breaches, and that agency ignored warnings from cybersecurity experts that its data systems were dangerously deficient and that there was substantial risk of imminent breach.

[27] Finance, Banking, and Credit**🔑 Identity theft in general**

Consumers, in putative class action, sufficiently alleged that third-parties' potential future criminal conduct of identity theft and fraud was reasonably foreseeable, and thus did not insulate credit reporting agency and related entities from liability for the future criminal conduct for purposes of consumers' tort claims in putative class action for, inter alia, negligence and negligence per se under Georgia law, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged that agency knew the likelihood and repercussions of cybersecurity threats and had stayed informed as to other well-publicized data breaches, and that agency had awareness of the risks that data breaches posed, including risks that compromise of personal information entailed.

[1 Cases that cite this headnote](#)

[28] Torts**🔑 Economic loss doctrine**

The economic loss rule, under Georgia law, generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort.

[29] Torts**🔑 Economic loss doctrine**

Under the economic loss rule, under Georgia law, a plaintiff may not recover in tort for purely economic damages arising from a breach of contract.

[30] Torts**🔑 Economic loss doctrine**

Where an independent duty exists under the law, under Georgia law the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule.

[31] Finance, Banking, and Credit**🔑 Identity theft in general**

Consumer reporting agency, as an entity that collected sensitive, private data from consumers and stored that data on its networks, had an independent duty to protect that personal information, and thus under Georgia law the economic loss rule did not apply to bar consumers' tort claims against agency and affiliated entities in putative class action for, inter alia, negligence and negligence per se, under Georgia law, arising from data breach in which personal and financial information of millions of Americans was potentially stolen.

[1 Cases that cite this headnote](#)

[32] Negligence**🔑 Elements in general**

In Georgia, a cause of action for negligence requires: (1) a legal duty to conform to a standard of conduct raised by the law for the protection of others against unreasonable risks of harm; (2) a

breach of this standard; (3) a legally attributable causal connection between the conduct and the resulting injury; and (4) some loss or damage flowing to the plaintiff's legally protected interest as a result of the alleged breach of the legal duty.

[33] Negligence

🔑 [Necessity and Existence of Duty](#)

The threshold issue in any cause of action for negligence, under Georgia law, is whether, and to what extent, the defendant owes the plaintiff a duty of care.

[34] Negligence

🔑 [Duty as question of fact or law generally](#)

Whether a duty that the defendant owes to the plaintiff exists, as required to support a negligence claim under Georgia law, is a question of law.

[35] Negligence

🔑 [Reasonable care](#)

Georgia law recognizes that one has a general duty to all the world not to subject them to an unreasonable risk of harm.

[36] Finance, Banking, and Credit

🔑 [Identity theft in general](#)

Consumers, in putative class action, sufficiently alleged that consumer reporting agency owed a legal duty to consumers to take reasonable precautions to safeguard the personal information in its custody, as required to state negligence claim under Georgia law against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged that agency knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

[37] Finance, Banking, and Credit

🔑 [Identity theft in general](#)

Consumers, in putative class action, failed to allege that consumer reporting agency voluntarily undertook a duty, as would support negligence claim under Georgia law against agency and affiliated entities, that was premised on agency voluntarily undertaking responsibility based on its purportedly unique position as one of three nationwide credit-reporting companies undertaking collection of highly sensitive information generally without consumers' knowledge or consent, arising from data breach in which personal and financial information of millions of Americans was potentially stolen.

[38] Negligence

🔑 [Violations of statutes and other regulations](#)

Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se.

[39] Negligence

🔑 [Violations of statutes and other regulations](#)

In order to make a negligence per se claim, under Georgia law, the plaintiff must show that it is within the class of persons intended to be protected by the statute and that the statute was meant to protect against the harm suffered.

[40] Antitrust and Trade Regulation

🔑 [Privacy](#)

The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission (FTC) Act. Federal Trade Commission Act § 5, 15 U.S.C.A. § 45(a).

[2 Cases that cite this headline](#)

[41] Finance, Banking, and Credit

🔑 [Actions](#)

Consumers, in putative class action, adequately stated claim against consumer reporting agency and affiliated entities for negligence per se under Georgia law, based on alleged violation of Federal Trade Commission (FTC) Act provision prohibiting unfair competition, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; complaint pleaded violation of FTC Act based on agency's purported failure to maintain reasonable and appropriate data security for consumers' sensitive personal information, and pleaded that consumers were within the class of persons intended to be protected by the FTC Act, and that the harm suffered was the kind the FTC Act was meant to protect against. Federal Trade Commission Act § 5, 15 U.S.C.A. § 45(a).

1 Cases that cite this headnote

[42] **Negligence**

🔑 [Violations of statutes and other regulations](#)

Under Georgia law, negligence per se is not liability per se.

[43] **Negligence**

🔑 [Violations of statutes or other regulations](#)

Negligence

🔑 [Necessity and Existence of Injury](#)

Even if negligence per se is shown, under Georgia law a plaintiff must still prove proximate causation and actual damage to recover on a claim of negligence per se.

[44] **Antitrust and Trade Regulation**

🔑 [Privacy](#)

The Georgia Fair Business Practices Act does not require businesses to safeguard personally identifiable information. [Ga. Code Ann. § 10-1-393.8](#).

[45] **Implied and Constructive Contracts**

🔑 [Unjust enrichment](#)

“Unjust enrichment,” under Georgia law, is an equitable doctrine that applies when as a matter of fact there is no legal contract, but where the party sought to be charged has been conferred a benefit by the party contending an unjust enrichment which the benefited party equitably ought to return or compensate for.

[46] **Implied and Constructive Contracts**

🔑 [Unjust enrichment](#)

In order to state a claim for unjust enrichment, under Georgia law, the plaintiffs must show that: (1) a benefit has been conferred; (2) compensation has not been given for receipt of the benefit; and (3) the failure to so compensate would be unjust.

[47] **Implied and Constructive Contracts**

🔑 [Unjust enrichment](#)

Consumers, whose personally identifiable information was provided to consumer services agency by third parties and not by consumers themselves, failed to show that they conferred a thing of value, namely their personally identifiable information, upon agency with the expectation that agency would be responsible for the cost, as required to state unjust enrichment claim under Georgia law against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen.

[48] **Implied and Constructive Contracts**

🔑 [Effect of Express Contract](#)

Under Georgia law, a party can only recover for a claim of unjust enrichment if there is not an express contract that governs the dispute.

[49] **Federal Civil Procedure**

🔑 [Alternate, Hypothetical and Inconsistent Claims](#)

While a party cannot recover under both a breach of contract and unjust enrichment theory under Georgia law, a plaintiff may plead these claims in the alternative.

[50] Federal Civil Procedure

➤ **Alternate, Hypothetical and Inconsistent Claims**

Consumers, who provided their personally identifiable information to credit services agency by, inter alia, obtaining credit monitoring services from agency, were able to allege claims for both breach of contract and unjust enrichment under Georgia law against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers were able to plead those claims in the alternative.

[51] Contracts

➤ **Merger in Subsequent Contract**

Under Georgia law, a merger clause operates as a disclaimer of all representations not made on the face of the contract.

[52] Finance, Banking, and Credit

➤ **Contracts**

Finance, Banking, and Credit

➤ **Financial Records and Privacy**

Even if consumer reporting agency's product agreement and terms of use contained valid merger clause, merger clause did not preclude breach of contract claims based on alleged breach of company's privacy policy under Georgia law in putative class action brought by consumers, who had purchased credit monitoring or identity theft protection services from agency, against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; terms of use provided that they were subject to conditions described on web site's privacy page.

[53] Finance, Banking, and Credit

➤ **Pleading**

Finance, Banking, and Credit

➤ **Actions**

Consumers in putative class action, who purchased credit monitoring or identity theft protection services from consumer reporting agency, did not explicitly allege that they read agency's privacy policy, or otherwise relied upon or were aware of representations and assurances made in privacy policy when choosing to use agency's services, and thus consumers did not allege mutual assent, as required to state breach of contract claim, based on purported breach of privacy policy as a standalone contract, under Georgia law against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen.

[54] Finance, Banking, and Credit

➤ **Judgment and relief**

Finance, Banking, and Credit

➤ **Monetary relief; damages**

Under express terms of contract consumers entered into with consumer reporting agency when purchasing credit monitoring or identity theft protection services from agency, agency would not be liable for damages for any use of or reliance upon information found on agency's web site, which included agency's privacy policy, and thus under terms of contract, consumers in putative class action were unable to seek damages for breach of contract under Georgia law against agency and affiliated entities based on alleged violation of the policy, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, even if agency's privacy policy was incorporated by reference into the contract.

[55] Finance, Banking, and Credit

➤ **Contracts**

Finance, Banking, and Credit

➤ **Financial Records and Privacy**

Consumer reporting agency's terms of use, which consumers agreed to when purchasing credit monitoring or identity theft protection services from agency, contained a valid merger clause, and thus consumers, in putative class action, were precluded from asserting claim for breach of implied contract under Georgia law against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen.

[56] Finance, Banking, and Credit

🔑 Pleading

Finance, Banking, and Credit

🔑 Actions

Consumers, in putative class action, who had purchased credit monitoring or identity theft protection services from agency, failed to allege mutual assent, as required to state claim against agency and affiliated entities for breach of implied contract under Georgia law, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers merely alleged that implied contract was formed since agency agreed to safeguard and protect consumers' personal information and to timely and accurately notify consumers if their personal information was breached or compromised, this allegation was a legal conclusion and not a factual allegation, and allegation failed to show that agency and consumers had a meeting of the minds.

[57] Contracts

🔑 Implied agreements

An implied contract, under Georgia law, only differs from an express contract in the type of proof used to prove its existence; the same element of mutual assent is required.

[58] Finance, Banking, and Credit

🔑 Actions

Consumers, in putative class action, adequately alleged that their out-of-state injuries fell within

ambit of many of the various state business fraud and consumer protection statutes that they brought claims under, as required for states to have authority to enforce its laws against consumer reporting agency and affiliated entities, that were located in Georgia, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, even if most consumers did not have direct commercial relationship with agency, if agency stored its data entirely on computers located in Georgia that were serviced by employees in Georgia, and if alleged acts and omissions occurred only in Georgia; consumers alleged that the acts within Georgia resulted in injuries in other states.

[59] Commerce

🔑 Regulation and conduct in general; particular businesses

Finance, Banking, and Credit

🔑 Identity theft in general

Various state business fraud and consumer protection statutes, under which consumers asserted claims in putative class action against consumer reporting agency and affiliated entities located in Georgia, did not involve economic protectionism and did not discriminate against out-of-state commerce, and thus Dormant Commerce Clause limitation, which provided that a statute that directly controls commerce occurring wholly outside the boundaries of a state exceeds inherent limits of that state's authority and is invalid, did not apply to preclude consumers' claims under the various statutes, arising from data breach in which personal and financial information of millions of Americans was potentially stolen. *U.S. Const. art. 1, § 8, cl. 3.*

[60] Federal Civil Procedure

🔑 Fraud, mistake and condition of mind

A complaint satisfies the rule requiring fraud claims to be pled with particularity if it sets forth precisely what statements or omissions were made in what documents or oral representations,

who made the statements, the time and place of the statements, the content of the statements and manner in which they misled the plaintiff, and what benefit the defendant gained as a consequence of the fraud. [Fed. R. Civ. P. 9\(b\)](#).

[61] Federal Civil Procedure

🔑 [Fraud, mistake and condition of mind](#)

Claims are only subject to the heightened pleading standards in the rule requiring claims alleging fraud be pleaded with particularity if they sound in fraud. [Fed. R. Civ. P. 9\(b\)](#).

[1 Cases that cite this headnote](#)

[62] Federal Civil Procedure

🔑 [Fraud, mistake and condition of mind](#)

A claim sounds in fraud, so as to be subject to the heightened pleadings standard in the rule requiring fraud claims to be pled with particularity, when a plaintiff alleges a unified course of fraudulent conduct and relies entirely on that course of conduct as the basis of that claim. [Fed. R. Civ. P. 9\(b\)](#).

[1 Cases that cite this headnote](#)

[63] Federal Civil Procedure

🔑 [Fraud, mistake and condition of mind](#)

In order for a claim to sound in fraud, so as to be subject to the heightened pleadings standard in the rule requiring fraud claims to be pled with particularity, the elements of the claim must be similar to that of common law fraud, requiring, among other things, proof of scienter, reliance, and injury. [Fed. R. Civ. P. 9\(b\)](#).

[1 Cases that cite this headnote](#)

[64] Federal Civil Procedure

🔑 [Fraud, mistake and condition of mind](#)

Consumer reporting agency and affiliated entities failed to show that the various state unfair and deceptive trade practice statutes, under which consumers brought claims in putative class action, sounded in fraud, as would require claims under the statutes to be

subject to heightened pleading standards of the rule requiring fraud claims to be pled with particularity, for purposes of consumers' claims arising from data breach in which personal and financial information of millions of Americans was potentially stolen; agency and entities did not show that the elements of the statutes were similar to the elements of common law fraud, and agency and entities did not show that consumers' theory of recovery rested upon a unified course of fraudulent conduct. [Fed. R. Civ. P. 9\(b\)](#).

[65] Finance, Banking, and Credit

🔑 [Actions](#)

Consumers, in putative class action, adequately alleged scienter, as required to state claims under various state fraud and consumer protection statutes against consumer reporting agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, where complaint provided a number of factual allegations demonstrating agency's knowledge and intent with regard to its cybersecurity, including that agency was aware of the importance of data security and of previous well-publicized data breaches, and that despite knowledge of cybersecurity risks agency sought to capitalize on increased number of breaches by providing identity theft protection instead of taking steps to improve deficiencies in its cybersecurity.

[66] Finance, Banking, and Credit

🔑 [Actions](#)

Consumers, in putative class action, adequately alleged cognizable injury, including ascertainable and monetary injury, as required to state claims under various state fraud and consumer protection statutes against consumer reporting agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen, where vast majority of consumers asserted that they spent money taking

steps to guard their identity, and some consumers alleged that they were victims of identity fraud.

[67] Finance, Banking, and Credit

🔑 **Actions**

Consumers' claims, in putative class action, under various state unfair and deceptive trade practices statutes which required a "consumer transaction," were not precluded on the basis that certain consumers did not allege that they engaged in a consumer transaction with consumer reporting agency, for purposes of claims under the statutes against agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen.

[68] Fraud

🔑 **Duty to disclose facts**

In the absence of a confidential relationship, no duty to disclose exists under Georgia law when parties are engaged in arm's-length business negotiations; in fact, an arm's-length relationship by its nature excludes a confidential relationship.

[69] Finance, Banking, and Credit

🔑 **Actions**

Consumers failed to allege that they were in a confidential relationship with consumer reporting agency, as required to support finding that consumer reporting agency had duty to disclose, and thus consumers failed to state claims against agency and affiliated entities under various state consumer-fraud statutes that imposed liability for omissions, based on agency allegedly having a duty to disclose due to statements it voluntarily made touting its cybersecurity, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; vast majority of consumers did not even allege that they were in an arms-length transaction with agency, and most of the consumers had no relationship with agency.

[70] Antitrust and Trade Regulation

🔑 **Fraud; deceit; knowledge and intent**

Finance, Banking, and Credit

🔑 **Monetary relief; damages**

Violation of the Illinois Personal Information Protection Act constitutes a violation of the Illinois Consumer Fraud and Deceptive Trade Practices Act, which expressly permits damages suits, and thus claims for violation of the Personal Information Protection Act can also seek recovery of monetary damages. 815 Ill. Comp. Stat. Ann. 505/1 et seq.; 815 Ill. Comp. Stat. Ann. 530/1 et seq.

[71] Action

🔑 **Statutory rights of action**

Antitrust and Trade Regulation

🔑 **Private entities or individuals**

There is a private right of action under the Massachusetts Consumer Protection Act. Mass. Gen. Laws Ann. ch. 93A, § 1 et seq.

[72] Action

🔑 **Statutory rights of action**

Antitrust and Trade Regulation

🔑 **Private entities or individuals**

There is a private right of action under the Nevada Deceptive Trade Practices Act. Nev. Rev. St. § 41.600(1).

[73] Antitrust and Trade Regulation

🔑 **Privacy**

There was no statutory basis under Georgia law for duty to safeguard personal information, as would support consumers' claims under Georgia Uniform Deceptive Trade Practices Act in putative class action against consumer reporting agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen. Ga. Code Ann. § 10-1-370 et seq.

[74] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

A private right of action exists under the Michigan data-breach statute. *Mich. Comp. Laws Ann.* §§ 445.72(13), 445.72(15).

[75] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

No private right of action exists under New York's data-breach statute. *N.Y. General Business Law* §§ 899-aa(6), 899-aa(9).

[76] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

No private of action exists under Connecticut's data-breach statute. *Conn. Gen. Stat. Ann.* § 36a-701b(g).

[77] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

A private right of action exists for violations of the Maryland Personal Information Protection Act through Maryland's Consumer Protection Act. *Md. Code Ann., Com. Law* § 13-101 et seq.; *Md. Code Ann., Com. Law* § 14-3508.

[78] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

A private right of action exists for violations of Montana's data-breach act through the Montana statute governing unfair business practices. *Mont. Code Ann.* §§ 30-14-103, 30-14-1705(3).

[79] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

New Jersey's data breach statute provides for a private right of action that can be enforced through New Jersey's consumer protection statute. *N.J. Stat. Ann.* §§ 56:8-163, 56:8-166.

[80] Action

🔑 Statutory rights of action

Finance, Banking, and Credit

🔑 Right of action; standing

There is no private right of action under the Georgia data-breach statute. *Ga. Code Ann.* § 10-1-912.

1 Cases that cite this headnote

[81] Finance, Banking, and Credit

🔑 Actions

Consumers, in putative class action against consumer reporting agency and affiliated entities, adequately alleged violation of various state data-breach statutes, for purposes of claims arising from data breach in which personal and financial information of millions of Americans was potentially stolen; statutes required notification to consumers, such as in the most expedient time possible and without unreasonable delay, and consumers alleged facts from which a jury could conclude that agency did not provide notice within a reasonable time, as notification statutes required.

[82] Social Security

🔑 Records, reports, and returns in general; disclosure

Consumer reporting agency and affiliated entities did not initiate transmission of Social Security numbers, so as to support consumers' claim in putative class action under the Maryland Social Security Number Privacy Act, arising

from data breach in which personal and financial information of millions of Americans was potentially stolen, where defendants suffered a criminal hack, and while defendants may have been negligent, consumers did not show that defendants initiated the transmission of their Social Security numbers, or engaged in any other conduct prohibit by the Act. [Md. Code Ann., Com. Law § 14-3402\(a\)](#).

[83] Finance, Banking, and Credit

🔑 **Actions**

Consumers, in putative class action, adequately alleged injury resulting from delay in notification, as required to state claims under various state data-breach statutes against consumer reporting agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged that they could have frozen their credit earlier, or taken other precautions to avoid misuse of their information.

[84] Federal Civil Procedure

🔑 **Consumers, purchasers, borrowers, and debtors**

Finance, Banking, and Credit

🔑 **Right of action; standing**

Consumers, in putative class action, sufficiently alleged that individuals nationwide, including individuals in Puerto Rico and the Virgin Islands, suffered injury from data breach, as required to state claims under laws of Puerto Rico and Virgin Islands against consumer reporting agency and affiliated entities, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged, and it was very likely, that there were consumers in Puerto Rico and the Virgin Islands whose personal information was compromised in the data breach.

[85] Costs

🔑 **Nature and Grounds of Right**

“Bad faith,” for purposes of the Georgia statute permitting an award of litigation expenses to a successful plaintiff where the defendant has acted in bad faith, is bad faith connected with the transaction and dealings out of which the cause of action arose, rather than bad faith in defending or resisting the claim after the cause of action has already arisen. [Ga. Code Ann. § 13-6-11](#).

[86] Costs

🔑 **Nature and Grounds of Right**

Bad faith, for purposes of the Georgia statute permitting an award of litigation expenses to a successful plaintiff where the defendant has acted in bad faith, requires more than bad judgment or negligence; rather the statute imports a dishonest purpose or some moral obliquity and implies conscious doing of wrong and a breach of known duty through some motive of interest of ill will. [Ga. Code Ann. § 13-6-11](#).

[87] Costs

🔑 **Nature and Grounds of Right**

Consumers, in putative class action, sufficiently alleged bad faith, as required to bring claim against consumer reporting agency and affiliated entities under Georgia statute permitting an award of litigation expenses to a successful plaintiff where defendant has acted in bad faith, arising from data breach in which personal and financial information of millions of Americans was potentially stolen; consumers alleged agency knew of severe deficiencies in cybersecurity and of serious threats to cybersecurity, but nonetheless declined to act on that knowledge. [Ga. Code Ann. § 13-6-11](#).

West Codenotes

Recognized as Unconstitutional

815 ILCS § 505-10a(a)

1308 CONSUMER CASES*OPINION AND ORDER**

THOMAS W. THRASH, JR., United States District Judge

This is a data breach case. It is before the Court on the Defendants' Motion to Dismiss the Consolidated Consumer Class Action Complaint [Doc. 425]. For the reasons set forth below, the Defendants' Motion to Dismiss the Consolidated Consumer Class Action Complaint [Doc. 425] is GRANTED in part and DENIED in part.

I. Background

On September 7, 2017, the Defendant Equifax Inc. announced that it was the subject of one of the largest data breaches in history.¹ From mid-May through the end of July 2017, hackers stole the personal and financial information of nearly 150 million Americans.² During this time period, Equifax failed to detect the hackers' presence in its systems, allowing the hackers to exfiltrate massive amounts of sensitive personal data that was in the company's custody.³ This data breach ("Data Breach") is unprecedented – it affected almost half of the entire American population.⁴ The Data Breach was also severe in terms of the type of information that the hackers were able to obtain. The hackers stole at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers.⁵ This is extremely sensitive personal information. Using this information, identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness.⁶

Equifax Inc. is a Georgia corporation with its principal place of business in Atlanta, ***1309** Georgia.⁷ Equifax is the parent company of the Defendants Equifax Information Services LLC and Equifax Consumer Services LLC.⁸ Both of those subsidiary companies are Georgia limited liability companies, with their principal places of business in Atlanta, Georgia.⁹ The Defendants operate together as an integrated consumer reporting agency.¹⁰ The Plaintiffs

are 96 consumers who allege that they have been injured by the Data Breach. They allege that they are suffering a "present, immediate, imminent, and continuing increased risk of harm" due to the compromise of their personally identifiable information in the Data Breach.¹¹ The Plaintiffs seek to represent a class of those similarly situated consumers in the United States who were injured by the Data Breach.¹²

Equifax's business model entails aggregating data relating to consumers from various sources, compiling that data into credit reports, and selling those reports to lenders, financial companies, employers, and others.¹³ Credit reporting agencies are "linchpins" of the nation's financial system due to the importance of credit reports in decisions to extend credit.¹⁴ Equifax also sells this information directly to consumers, allowing consumers to purchase their credit files and credit scores.¹⁵ In recent years, Equifax has worked to rapidly grow its business. Recognizing the value in obtaining massive troves of consumer data, Equifax has aggressively acquired companies with the goal of expanding into new markets and acquiring new sources of data.¹⁶ Equifax now maintains information on over 820 million individuals and 91 million businesses worldwide.¹⁷

Equifax recognized the importance of data security, and the value of the data in its custody to cybercriminals. Equifax observed other major, well-publicized data breaches, including those at Target, Home Depot, Anthem, and its competitor Experian.¹⁸ Equifax held itself out as a leader in confronting such threats, offering "data breach solutions" to businesses.¹⁹ It also acquired two identity theft protection companies, Trusted ID and ID Watchdog.²⁰ Equifax was also the subject of several prior data breaches. From 2010 on, Equifax suffered several different data breach incidents highlighting deficiencies in its cybersecurity protocol.²¹ Given these prior breaches, cybersecurity experts concluded that Equifax was susceptible to a major data breach.²² Analyses of Equifax's cybersecurity demonstrated that it lacked basic maintenance techniques that are ***1310** highly relevant to potential data breaches.²³ However, despite these risks, Equifax did little to improve its cybersecurity practices. Equifax's leaders afforded low priority to cybersecurity, spending a small fraction of the company's budget on cybersecurity.²⁴

The story of the Data Breach begins on March 6, 2017. On that date, a serious vulnerability in the Apache Struts software was discovered and reported.²⁵ This software, a popular open-source program, was used by Equifax in its consumer dispute portal website.²⁶ The next day, the Apache Software Foundation issued a free patch and urged all users to immediately implement the patch.²⁷ The Department of Homeland Security also issued warnings concerning this vulnerability.²⁸ Equifax internally disseminated the warning, but never implemented the patch.²⁹ Then, beginning on May 13, 2017, hackers were able to manipulate the Apache Struts vulnerability to access Equifax's systems, and using simple commands determined the credentials of network accounts that allowed them to access the confidential information of millions of American consumers.³⁰ From May 13 to July 30, 2017, the hackers remained undetected in Equifax's systems.³¹ During this time, the hackers were able to steal the sensitive personally identifiable information of approximately 147.9 million American consumers.³² The personally identifiable information that hackers obtained in the Data Breach includes names, addresses, birth dates, Social Security numbers, driver's license information, telephone numbers, email addresses, tax identification numbers, credit card numbers, credit report dispute documents, and more.³³

On July 29, 2017, Equifax's security team noticed "suspicious network traffic" in the dispute portal.³⁴ The next day, the consumer dispute portal was deactivated and taken offline.³⁵ On July 31, 2017, Equifax's CEO Richard Smith was informed of the breach.³⁶ On August 2, 2017, Equifax informed the Federal Bureau of Investigation about the Data Breach, and retained legal counsel to guide its investigation.³⁷ Equifax also hired cybersecurity firm Mandiant to investigate the suspicious activity.³⁸ On September 7, 2017, seven weeks after discovering suspicious activity, Equifax publicly disclosed the Data Breach in a press release.³⁹ Experts have since opined that the Data Breach was the result of weak cybersecurity measures and Equifax's low priority for data security.⁴⁰

***1311** The Plaintiffs here are a putative class of consumers whose personal information was stolen during the Data Breach. The class alleges that it has been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of

the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. The putative class brings a number of nationwide claims, along with a number of state claims. The class also seeks declaratory and injunctive relief. The Defendants now move to dismiss.

II. Legal Standard

[1] [2] [3] A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief.⁴¹ A complaint may survive a motion to dismiss for failure to state a claim, however, even if it is "improbable" that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely "remote and unlikely."⁴² In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff.⁴³ Generally, notice pleading is all that is required for a valid complaint.⁴⁴ Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests.

III. Discussion

A. Choice of Law

[4] [5] [6] First, the Court concludes that Georgia law governs this case. This case is before the Court based on diversity jurisdiction. The Court therefore looks to Georgia's choice of law rules to determine the appropriate rules of decision.⁴⁵ Georgia follows the traditional approach of *lex loci delicti* in tort cases, which generally applies the substantive law of the state where the last event occurred necessary to make an actor liable for the alleged tort.⁴⁶ Usually, this means that the "law of the place of the injury governs rather than the law of the place of the tortious acts allegedly causing the injury."⁴⁷ However, there is an exception when the law of the foreign state is the common law. "[T]he application ***1312** of another jurisdiction's laws is limited to statutes and decisions construing those statutes. When no statute is involved, Georgia courts apply the common law as developed in Georgia rather than foreign case law."⁴⁸ The Plaintiffs identify no foreign statutes that govern their common law claims. Therefore, the Court will apply Georgia law to the common law claims.⁴⁹

B. Fair Credit Reporting Act

The Defendants first move to dismiss the Consumer Plaintiffs' claims under the Fair Credit Reporting Act ("FCRA"). Under the FCRA, a "consumer reporting agency may furnish a consumer report" only under limited circumstances provided for in the statute.⁵⁰ In Count 1 of the Complaint, the Consumer Plaintiffs allege that the Defendants "furnished Class members' consumer reports" in violation of section 1681b of the FCRA and "failed to maintain reasonable procedures designed to limit the furnishing of Class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of Class members' consumer reports to unauthorized entities or computer hackers" in violation of section 1681e of the FCRA.⁵¹ The Defendants move to dismiss, arguing that Equifax did not "furnish" any consumer information within the meaning of the statute, and that the stolen personally identifying information is not a "consumer report" within the meaning of the statute.⁵² They also argue that since the Consumer Plaintiffs' section 1681b claim fails to state a claim, their section 1681e also necessarily fails.⁵³ The Court agrees that the Consumer Plaintiffs fail to state a claim under the FCRA.

[7] First, the Defendants argue that Equifax did not "furnish" the Plaintiffs' personal information within the meaning of the FCRA. The FCRA provides that a consumer reporting agency may only "furnish" a consumer report under limited circumstances.⁵⁴ However, the statute does not further define "furnish." Generally, courts have held that information that is stolen from a credit reporting agency is not "furnished" within the meaning of the FCRA. For example, in *In re Experian Data Breach Litigation*, the court explained that "[a]lthough 'furnish' is not defined in the FCRA, courts generally use the term to describe the active transmission of information to a third-party rather *1313 than a failure to safeguard the data."⁵⁵ In such a case, the data is stolen by a third party, and not furnished to the third party.⁵⁶ Other courts have come to the same conclusion.⁵⁷ The Plaintiffs acknowledge that the caselaw supports Equifax's argument, but contend nonetheless that Equifax's conduct was "so egregious" that it should be considered akin to furnishing.⁵⁸ The Plaintiffs fail to offer a discernable criteria by which to determine when conduct becomes so egregious that it becomes akin to furnishing. Even assuming Equifax's conduct was egregious,

the Court concludes that the Plaintiffs have not alleged facts showing that Equifax "furnished" the Plaintiffs' consumer reports to the hackers.

[8] Next, the Defendants argue that the personally identifying information stolen during the Data Breach is not a "consumer report" within the meaning of the FCRA.⁵⁹ The Court agrees. Section 1681b of the FCRA prohibits the furnishing of "consumer reports," except under limited circumstances.⁶⁰ The FCRA defines "consumer report," in general, to mean:

[A]ny written, oral, or other communication of any information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for--(A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.⁶¹

Equifax argues – and the Plaintiffs do not dispute this – that the hackers did not obtain access to the active credit files maintained by one of the Equifax subsidiaries. The hackers got only "legacy" data. Courts, facing similar factual circumstances, have concluded that information such as that taken in the Data Breach does not constitute a "consumer report," but instead is "header information."⁶² Such information is not a "consumer report" because it does not bear on an individual's credit worthiness.⁶³ Information, such as a consumer's "name, phone number, social security number, date of birth, driver's license, current address, and time spent at that address" does not, itself, constitute *1314 such a credit report.⁶⁴ The Plaintiffs' argument that the information stolen in the Data Breach could bear on their credit worthiness is not persuasive. Therefore, the Court

concludes that the Plaintiffs fail to allege facts showing that the information stolen was a “credit report.”

[9] Finally, since the Consumer Plaintiffs' [section 1681b](#) claim fails, their [section 1681e](#) claim must also necessarily fail. [Section 1681e](#) requires consumer reporting agencies to “maintain reasonable procedures designed to avoid violations of [section 1681c](#) of this title and to limit the furnishing of consumer reports to the purposes listed under [section 1681b](#) of this title.”⁶⁵ However, a plaintiff bringing a claim that a reporting agency violated the “reasonable procedures” requirement of [section 1681e](#) must first show that the reporting agency released the report in violation of [section 1681b](#).⁶⁶ Therefore, since the Plaintiffs' claims under [section 1681b](#) fail, their claims under [section 1681e](#) also fail.

[10] Next, two Plaintiffs, Grace Cho and Debra Lee, bring claims under [15 U.S.C. § 1681g\(a\)](#).⁶⁷ These Plaintiffs, referred to as the “FCRA Disclosure Subclass” in the Complaint, allege that the Defendants violated [sections 1681\(a\)\(1\)](#) and [1681\(a\)\(3\)](#) of the FCRA by failing to clearly and accurately disclose all of the information in their consumer files after requesting Equifax to do so.⁶⁸ According to these Plaintiffs, the Defendants violated this statute by failing to identify the Data Breach and the individuals who procured their information, namely the hackers.⁶⁹ However, as explained above, the hackers did not obtain a “consumer report” within the meaning of the FCRA. And Equifax could not be expected to disclose the identity of the unknown hackers. Therefore, this claim should be dismissed.

C. Legally Cognizable Injury

The Defendants next argue that all of the Plaintiffs' tort claims, including their negligence, negligence per se, and state consumer protection act violations, fail because they have not sufficiently alleged injury and proximate causation.⁷⁰ According to the Defendants, the Plaintiffs' injuries are not legally cognizable harms, and even if they were, the Plaintiffs have failed to adequately allege that the Defendants proximately caused their harms.⁷¹ Finally, the Defendants argue that the Plaintiffs' tort claims are all barred by the economic loss doctrine.

*1315 1. Non-Harms and Speculative Future Harms

[11] [12] First, the Defendants contend that the Plaintiffs have not pleaded legally cognizable harms because their purported injuries only include “non-harms” and “speculative future harms.”⁷² “It is well-established Georgia law that before an action for a tort will lie, the plaintiff must show he sustained injury or damage as a result of the negligent act or omission to act in some duty owed to him.”⁷³ “Although nominal damages can be awarded where there has been an injury but the injury is small, ... where there is no evidence of injury accompanying the tort, an essential element of the tort is lacking, thereby entitling the defendant to judgment in his favor.”⁷⁴

[13] The Defendants first contend that the compromise of personally identifiable information itself is not an injury.⁷⁵ Each of the Plaintiffs alleges that his or her personally identifiable information was compromised in the Data Breach.⁷⁶ Such an injury is legally cognizable under Georgia law.⁷⁷ The cases relied upon by the Defendants are distinguishable. The Defendants cite *Rite Aid of Georgia, Inc. v. Peacock* for the proposition that a plaintiff suffers no injury from the illegal sale of personally identifiable information.⁷⁸ However, as the Plaintiffs point out, the plaintiff in that case did not allege that this information was misused, or likely to be misused.⁷⁹ In *Rite Aid*, the plaintiff's pharmacy records were sold from Rite Aid to Walgreens when a Rite Aid store was closing.⁸⁰ The plaintiff sought certification of a class of all individuals whose information had been sold to Walgreens.⁸¹ The court concluded that class certification was not proper, in part, because the plaintiff had not alleged an injury from the sale of his information from one pharmacy to the other, and instead only alleged a violation of law.⁸² In contrast, the Plaintiffs here have alleged that they have been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. These allegations of actual injury are sufficient to support a claim for relief.⁸³

*1316 The Defendants also cite *Finnerty v. State Bank & Trust Company* for the proposition that fear of future damages from identity theft is too speculative to form a basis of recovery.⁸⁴ However, as the Plaintiffs emphasize, that case involved an invasion of privacy claim by an individual

whose Social Security number was included in a public court filing.⁸⁵ The court concluded that this claim failed because, to state a claim for invasion of privacy, a plaintiff must show that there was a public disclosure in which information is distributed to the public at large.⁸⁶ There, the claimant failed to allege that anyone actually saw his Social Security number, and thus did not prove that there was a public disclosure.⁸⁷ Thus, the court there did not hold that the disclosure of personal information is, as a matter of law, not a legally cognizable injury. Instead, it concluded that one of the elements of an invasion of privacy claim was not met, making it distinguishable from this case.⁸⁸ And, in contrast to the inadvertent disclosure of a Social Security number in a single public court filing, the compromise of a huge amount of personally identifying information by criminal hackers presents a much more significant risk of identity fraud.

The Defendants also cite *Randolph v. ING Life Insurance and Annuity Company*.⁸⁹ There, the plaintiffs sued after a laptop computer containing their personal information was stolen from the home of one of the defendant's employees, alleging that there was a substantial risk of identity theft and other dangers due to the possible unauthorized use of their personal information.⁹⁰ In that case, there was no evidence that the theft occurred for the specific purpose of obtaining the information on the laptop as opposed to the computer itself. Here, by contrast, the Plaintiffs allege that their information was specifically targeted and has already been misused. The Plaintiffs have adequately alleged facts showing actual cognizable injury.

The Defendants also cite *Collins v. Athens Orthopedic Clinic* in their reply brief.⁹¹ There, the defendant's patients sued after a cyberhacker stole their personal information from the defendant's systems.⁹² The court concluded that the plaintiffs did not allege a legally cognizable harm.⁹³ It explained that:

Plaintiffs allege that their information has been compromised and that they have spent time placing fraud or credit alerts on their accounts and “anticipate” spending more time on these activities. Plaintiffs claim damages, specifying only the cost of identity theft protection, credit monitoring, and credit freezes to be maintained “over the course of a *1317 lifetime.” While credit monitoring and other precautionary measures are undoubtedly prudent, we find that they are not recoverable damages on the facts

before us because Plaintiffs seek only to recover for an increased risk of harm.⁹⁴

Thus, according to the Defendants, the Plaintiffs' claims must fail, since costs associated with protecting the plaintiffs' personal information in *Collins* failed to establish a sufficient injury.⁹⁵

However, *Collins* is distinguishable. There, the plaintiffs alleged only an “increased risk of harm” associated with taking precautionary measures.⁹⁶ The mere risk of harm, and not the type of injuries alleged, led the court to conclude that the plaintiffs' allegations as to injuries failed. In contrast, the Plaintiffs here have not pleaded merely an increased risk of harm. Instead, they have alleged that they have already incurred significant costs in response to the Data Breach. Many of the Plaintiffs have also already suffered forms of identity theft. Moreover, the Plaintiffs here have sufficiently alleged a substantial and imminent risk of impending identity fraud due to the vast amount of information that was obtained in the Data Breach. The Court concludes that these allegations are sufficient.

[14] The Defendants also argue that the Plaintiffs that allege payment card fraud have failed to allege a sufficient injury.⁹⁷ Plaintiffs Alvin Alfred Kleveno Jr., Maria Martucci, and Robert J. Etten allege that they experienced unauthorized charges on their payment cards as a result of the Data Breach.⁹⁸ The Defendants contend that these allegations are insufficient because these Plaintiffs have not alleged the date on which these fraudulent charges were made, and because they failed to allege that they were not reimbursed for those charges.⁹⁹ However, under Rule 8's requirement of a plain and simple statement, these Plaintiffs need not allege the specific date on which these fraudulent charges occurred. The Plaintiffs' allegations that such charges occurred are sufficient, and the Defendants cite no authority holding otherwise. Furthermore, contrary to the Defendants' assertions, these Plaintiffs also need not allege that they were not reimbursed for these fraudulent charges to adequately allege an injury.¹⁰⁰ The Plaintiffs' allegations that they suffered unauthorized charges on their payment cards as a result of the Data Breach are actual, concrete injuries that are legally cognizable under Georgia law.

2. Proximate Causation

[15] [16] [17] [18] [19] The Defendants next contend that the Plaintiffs have failed to adequately allege that Equifax proximately caused their injuries.¹⁰¹ “[B]efore any negligence, even if proven, can be actionable, that *1318 negligence must be the proximate cause of the injuries sued upon.”¹⁰² “To establish proximate cause, a plaintiff must show a legally attributable causal connection between the defendant’s conduct and the alleged injury.”¹⁰³ A plaintiff must establish “that it is more likely than not that the conduct of the defendant was a cause in fact of the result.”¹⁰⁴ “A mere possibility of such causation is not enough; and when the matter remains one of pure speculation or conjecture, or the probabilities are at best evenly balanced, it becomes the duty of the court to grant summary judgment for the defendant.”¹⁰⁵

[20] First, the Defendants argue that the Plaintiffs fail to allege that any injuries resulting from identity theft, payment-card fraud, or other similar theories resulted specifically from the Equifax Data Breach, and not some other data breach or fraudulent conduct.¹⁰⁶ According to the Defendants, the Plaintiffs highlight dozens of other security breaches dating to 2013 in the Complaint, and the Defendants assert that over 1,500 data breaches occurred in 2017 alone. Thus, since the Plaintiffs have failed to allege that their injuries resulted directly from their personal information being obtained in this specific Data Breach, their theory of causation is “guesswork at best.”¹⁰⁷

However, the Court finds this argument unpersuasive. Many of the Plaintiffs have alleged in the Complaint that they suffered some form of identity theft or other fraudulent activity as a result of the Data Breach.¹⁰⁸ Such an allegation is sufficient at the pleading stage to establish that the Data Breach was the proximate cause of this harm. The Plaintiffs need not explicitly state that other breaches did *not* cause these alleged injuries, since their allegations that this Data Breach *did* cause their injuries implies such an allegation. Furthermore, allowing the Defendants “to rely on other data breaches to defeat a causal connection would ‘create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable.’ ”¹⁰⁹ The Court declines to create such a perverse incentive.

Many of the Plaintiffs also allege in the Complaint that they purchased credit monitoring and incurred other costs in

direct response to the Data Breach.¹¹⁰ Thus, even assuming their identity theft injuries *1319 resulted from previous breaches, these separate injuries resulted only from the occurrence of the Data Breach. Finally, even assuming that such an argument could disprove proximate causation, it presents a factual dispute most appropriate for a jury to consider. The Plaintiffs have alleged that the Data Breach caused their identities to be stolen, while the Defendants contend prior breaches caused these injuries. This is purely a dispute of fact that is not appropriate for resolution at this stage of the litigation.¹¹¹ Therefore, the Court concludes that the Plaintiffs have adequately alleged that the Data Breach proximately caused their injuries. The Plaintiffs plausibly allege that Equifax had custody of their personally identifiable information, that Equifax’s systems were hacked, that these hackers obtained this personal information, and that as a result of this breach, they have become the victims of identity theft and other fraudulent activity. This is sufficient.

[21] [22] Next, the Defendants contend that the Plaintiffs’ injuries were proximately caused by an “unidentified third party’s criminal acts,” and not Equifax itself.¹¹² According to the Defendants, the unforeseeable criminal acts of third parties “insulate” defendants from liability.¹¹³ “Generally, there is no duty to prevent the unforeseeable ‘intervening criminal act of a third person.’ ”¹¹⁴ Under Georgia law, “when a defendant claims that its negligence is not the proximate cause of the plaintiff’s injuries, but that an act of a third party intervened to cause those injuries, the rule is ‘that an intervening and independent wrongful act of a third person producing the injury, and without which it would not have occurred, should be treated as the proximate cause, insulating and excluding the negligence of the defendant.’ ”¹¹⁵

[23] [24] [25] However, “this rule does not insulate the defendant ‘if the defendant had reasonable grounds for apprehending that such wrongful act would be committed.’ ”¹¹⁶ “[I]f the character of the intervening act claimed to break the connection between the original wrongful act and the subsequent injury was such that its probable or natural consequences could reasonably have been anticipated, apprehended, or foreseen by the original wrong-doer, the causal connection is not broken, and the original wrong-doer is responsible for all of the consequences resulting from the intervening act.”¹¹⁷ Thus, if the Defendants had reasonable grounds to anticipate the criminal act, then they are not insulated from liability. “In determining whether

a third party criminal act is foreseeable, Georgia ^{*1320} courts have held that ‘the incident causing the injury must be substantially similar in type to the previous criminal activities ... so that a reasonable person would take ordinary precautions to protect his or her customers or tenants against the risk posed by that type of activity.’ ”¹¹⁸ The question of reasonable foreseeability of a criminal attack is generally for a jury to determine.¹¹⁹ However, it may not be in this case because of the many public statements by Equifax that it knew how valuable its information was to cyber criminals and its susceptibility to hacking attempts.

In *Home Depot*, this Court allowed a negligence claim premised upon a data breach to continue, noting that the defendant “knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it.”¹²⁰ Similarly, in *Arby’s*, the court noted that the defendant knew about potential data breach threats but failed to implement reasonable security measures.¹²¹ Thus, according to the court, the criminal acts of the cyberhackers were reasonably foreseeable, and thus the plaintiffs’ negligence claims could proceed.¹²² In *Arby’s*, the court compared criminal data breaches to the “peculiarly similar context of premises liability,” where the Georgia Supreme Court has held that if a proprietor “has reason to anticipate a criminal act,” then he or she has a duty to “exercise ordinary care to guard against injury from dangerous characters.”¹²³

[26] The Court concludes that, as in *Arby’s* and *Home Depot*, the criminal acts of the hackers were reasonably foreseeable to the Defendants, and thus do not insulate them from liability. In the Complaint, the Plaintiffs allege that the Defendants observed major data breaches at other corporations, such as Target, Anthem, and Experian.¹²⁴ Equifax itself even experienced prior data breaches.¹²⁵ Furthermore, Equifax ignored warnings from cybersecurity experts that its data systems were dangerously deficient, and that there was a substantial risk of an imminent breach.¹²⁶ These allegations are sufficient to establish that the acts of the third party cyberhackers were reasonably foreseeable. Thus, the causal chain is not broken.

[27] The Defendants also assert that future identity theft and fraud is a second intervening cause that insulates them from liability.¹²⁷ According to the Defendants, the Plaintiffs have not pleaded that this fraudulent conduct is the

probable consequence of a data breach, and thus was not foreseeable. However, the Court concludes that the Plaintiffs have adequately alleged that such conduct was reasonably foreseeable. In the Complaint, the Plaintiffs allege ^{*1321} that the Defendants knew the “likelihood and repercussions” of cybersecurity threats, and had stayed informed as to other well-publicized breaches.¹²⁸ The Complaint details the Defendants’ alleged awareness of the risks that data breaches pose, including the risks that the compromise of personal information entails.¹²⁹ Equifax knew that fraudulent activity had resulted from other, well-publicized data breaches.¹³⁰ Thus, the Plaintiffs have adequately alleged that this criminal conduct was reasonably foreseeable.

3. Economic Loss Doctrine

[28] [29] [30] [31] The Defendants next argue that the economic loss doctrine bars the Plaintiffs’ tort claims.¹³¹ “The ‘economic loss rule’ generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort.”¹³² In other words, “a plaintiff may not recover in tort for purely economic damages arising from a breach of contract.”¹³³ Where, however, “an independent duty exists under the law, the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule.”¹³⁴ Here, the independent duty exception would bar application of the economic loss rule. “It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]”¹³⁵ As discussed below, the Defendants owed the Plaintiffs a duty of care to safeguard their personal information. Therefore, since an independent duty existed, the economic loss rule does not apply.

D. Negligence

Next, the Defendants move to dismiss the Plaintiffs’ negligence claim.¹³⁶ In Count 2 of the Complaint, the Plaintiffs allege that Equifax owed a duty to the Plaintiffs to “exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons.”¹³⁷ The Plaintiffs also allege that Equifax had a duty of care that

arose from Section 5 of the Federal Trade Commission Act (the “FTC Act”), and the FCRA.¹³⁸ The Defendants contend that they were under no duty of care toward the Plaintiffs.¹³⁹

*1322 [32] [33] [34] [35] In Georgia, “[a] cause of action for negligence requires (1) [a] legal duty to conform to a standard of conduct raised by the law for the protection of others against unreasonable risks of harm; (2) a breach of this standard; (3) a legally attributable causal connection between the conduct and the resulting injury; and, (4) some loss or damage flowing to the plaintiff’s legally protected interest as a result of the alleged breach of the legal duty.”¹⁴⁰ “The threshold issue in any cause of action for negligence is whether, and to what extent, the defendant owes the plaintiff a duty of care.”¹⁴¹ Whether such a duty exists is a question of law.¹⁴² Georgia recognizes a general duty “to all the world not to subject them to an unreasonable risk of harm.”¹⁴³

The Defendants contend that Georgia law does not impose a duty of care to safeguard personal information.¹⁴⁴ The Defendants rely primarily upon a recent Georgia Court of Appeals case, *McConnell v. Georgia Department of Labor*.¹⁴⁵ In *McConnell*, the plaintiff filed a class action against the Georgia Department of Labor after one of its employees sent an email to 1,000 Georgians who had applied for unemployment benefits.¹⁴⁶ This email included a spreadsheet with the name, Social Security number, phone number, email address, and age of 4,000 Georgians who had registered for services with the agency.¹⁴⁷ The plaintiff, whose information was disclosed, filed a class action, asserting, among other claims, a claim for negligence.¹⁴⁸

A brief overview of *McConnell’s* procedural history is helpful in understanding the court’s decision in that case. In June 2016, the Georgia Court of Appeals initially rejected the plaintiff’s claims.¹⁴⁹ In *McConnell I*, the plaintiff, recognizing that such a duty had not been expressly recognized in Georgia caselaw, contended that such a duty arose from two statutory sources.¹⁵⁰ The court concluded that neither of these statutory sources gave rise to a duty to safeguard personal information.¹⁵¹ The court explained that “McConnell’s complaint is premised on a duty of care to safeguard personal information that has no source in Georgia statutory law or caselaw and that his complaint therefore failed to state a claim of negligence.”¹⁵² However, in doing so, the court expressly distinguished this Court’s prior holding

in *Home Depot*, noting that this *1323 Court “found a duty to protect the personal information of the defendant’s customers in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies” and explaining that “[t]here are no such allegations in this case.”¹⁵³

Then, the Georgia Supreme Court vacated *McConnell I*, holding that the Court of Appeals could not decide whether the plaintiff failed to state a claim without first considering whether the doctrine of sovereign immunity barred his claims.¹⁵⁴ On remand, the Georgia Court of Appeals, after deciding that sovereign immunity did not bar the plaintiff’s claims, once again concluded that the plaintiff’s negligence claim failed because “McConnell’s complaint is premised on a duty of care to safeguard personal information that has no source in Georgia statutory law or caselaw and that his complaint therefore failed to state a claim of negligence.”¹⁵⁵ Examining both the Georgia Personal Identity Protection Act and the Georgia Fair Business Practices Act, the court concluded that neither gave rise to a duty to safeguard personal information.¹⁵⁶ Although the legislature showed a “concern about the cost of identity theft to the marketplace” through these statutes, it did not act to “establish a standard of conduct intended to protect the security of personal information, as some other jurisdictions have done in connection with data protection and data breach notification laws.”¹⁵⁷

The Defendants contend that *McConnell III* confirms that there is no duty under Georgia law, common law or statutory, to safeguard personally identifiable information.¹⁵⁸ The Georgia Supreme Court has granted certiorari in the case. The Defendants, at oral argument, asked the Court to delay ruling upon the Motion to Dismiss until a ruling by the Georgia Supreme Court. However, it seems very unlikely to me that the Georgia Supreme Court will adopt a rule of law that tells hundreds of millions of consumers in the United States that a national credit reporting agency headquartered in Georgia has no obligation to protect their confidential personal identifying data. Unlike the Georgia Department of Labor, Equifax and the other national credit reporting agencies are heavily regulated by federal law. As noted previously, the Fair Credit Reporting Act strictly limits the circumstances under which a credit reporting agency may disclose consumer

credit information.¹⁵⁹ The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.¹⁶⁰ The Gramm–Leach–Bliley Act *1324 required the FTC to establish standards for financial institutions to protect consumers' personal information.¹⁶¹ The FTC has done that.¹⁶²

The Plaintiffs contend that, under Georgia law, allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish a duty of care.¹⁶³ The Plaintiffs rely primarily upon *Home Depot* and *Arby's* for this proposition. In *Home Depot*, this Court denied the defendant's motion to dismiss a negligence claim arising out of a data breach.¹⁶⁴ The Court concluded that Home Depot had a duty to safeguard customer information because it “knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it.”¹⁶⁵ The Court, citing the Georgia Supreme Court's decision in *Bradley Center, Inc. v. Wessner*, came to this conclusion by expounding upon the general duty to “all the world not to subject them to an unreasonable risk of harm.”¹⁶⁶ The Court noted that “to hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk.”¹⁶⁷

Then, in *Arby's*, the court declined to dismiss a plaintiff's negligence claim arising out of a data breach. The court explained that “[u]nder Georgia law and the standard articulated in *Home Depot*, allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss.”¹⁶⁸ The court held that Arby's was under a duty to safeguard its customers' personal data due to allegations that it knew about potential problems and failed to implement reasonable security measures, knew about other highly-publicized data breaches, and was aware that its parent company had suffered a significant breach using the same computer system.¹⁶⁹ The *Arby's* court also distinguished *McConnell I*, explaining that it was not “expressly inconsistent” with *Home Depot* because *Home Depot* found a duty to protect personal information in the context of the defendant's failure to implement reasonable

security measures to combat a foreseeable risk, while there were no such allegations in *McConnell I*.¹⁷⁰ The court also explained that the *McConnell I* court's characterization of *Wessner* as a narrow holding did not change its conclusion since *McConnell I* did not change the general duty that arises from foreseeable criminal *1325 acts.¹⁷¹

The parties' interpretations of this caselaw diverge greatly. The Defendants contend that *McConnell III*, the latest decision of all of these cases, clarified this caselaw and affirmatively stated that there is no duty to safeguard personal information.¹⁷² Thus, according to the Defendants, *Home Depot* and *Arby's* are no longer good law.¹⁷³ The Plaintiffs, in turn, argue that due to the factual differences between *McConnell III*, on the one hand, and *Arby's* and *Home Depot*, on the other hand, *McConnell III* does not conflict with these two cases.¹⁷⁴ According to the Plaintiffs, there were no allegations in *McConnell III* that the state agency should have known that its employee would inadvertently disclose this personal information. In contrast, *Home Depot* and *Arby's* premised their holdings on the detailed allegations that the data breaches were foreseeable.¹⁷⁵ Finally, the Plaintiffs argue that, despite the Defendants' characterizations, they are not asking this Court to recognize a new duty under Georgia law, but instead are asking it to apply traditional tort and negligence principles to the facts of this case.¹⁷⁶

[36] The Court concludes that, under the facts alleged in the Complaint, Equifax owed the Plaintiffs a duty of care to safeguard the personal information in its custody. This duty of care arises from the allegations that the Defendants knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures. *McConnell III* does not alter this conclusion. As the court in *McConnell I* noted, a critical distinction between these cases is that the duty in *Home Depot* arose from allegations that the defendant failed to implement reasonable security measures in the face of a known security risk.¹⁷⁷ Such allegations did not exist in the *McConnell* line of cases.¹⁷⁸ The *McConnell III* court came to the same conclusion as the *McConnell I* court, and did nothing to dispel this distinction made in *McConnell III*. Furthermore, given this mention of *Home Depot* in *McConnell I*, and the court's subsequent holding in *Arby's*, the *McConnell III* court's silence on this issue suggests a tacit approval of this distinction. And, as this Court noted in *Home Depot*, to hold otherwise would create perverse incentives for businesses

who profit off of the use of consumers' personal data to turn a blind eye and ignore known security risks.¹⁷⁹

The Defendants go to great lengths to distinguish the Georgia Supreme Court's decision in *Bradley Center, Inc. v. Wessner*. Both *Home Depot* and *Arby's* relied, in part, upon *Wessner* to conclude that the defendants were under a duty to take reasonable measures to avoid a foreseeable risk of harm from a data breach incident. In *Wessner*, a man who voluntarily committed *1326 himself to a psychiatric hospital made statements to the hospital's staff that he desired to harm his wife.¹⁸⁰ Despite these statements, the man was issued a weekend pass by the staff, and he subsequently obtained a gun, confronted his wife and another man, and killed them both.¹⁸¹ The Georgia Supreme Court concluded that the hospital owed a duty of care to the man's wife.¹⁸² The court explained that “[t]he legal duty in this case arises out of the general duty one owes to all the world not to subject them to an unreasonable risk of harm.”¹⁸³

The Defendants argue that the holding in *Wessner* is much narrower than this. According to them, *Wessner* merely stands for the narrow proposition that a physician owes a legal duty when, in the course of treating a mental health patient, that physician exercises control over the patient and knows or should know that the patient is likely to cause harm to others. The Defendants further assert that the *Wessner* court's references to general negligence principles were done in an effort to explain why the case was a negligence case, and not a medical malpractice case. However, despite the Defendants' efforts to minimize the importance of *Wessner*, the Court finds that *Wessner* supports the conclusion that the Defendants owed a legal duty to take reasonable measures to prevent a reasonably foreseeable risk of harm due to a data breach incident. Nowhere in the *Wessner* decision does the Georgia Supreme Court limit its holding to the narrow proposition that the Defendants assert. In fact, in *Wessner*, the court explained that it was not creating a “new tort,” but instead that it was applying “our traditional tort principles of negligence to the facts of this case.”¹⁸⁴ Other Georgia cases have similarly applied these same general principles.¹⁸⁵ Likewise, this Court concludes that, under traditional negligence principles, the Defendants owed a legal duty to the Plaintiffs to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident.

[37] The Defendants then argue that they did not “voluntarily” undertake a duty.¹⁸⁶ In the Complaint, the Plaintiffs allege that Equifax's duty also arose from its “unique position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system” and that Equifax “undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers.”¹⁸⁷ The Defendants contend that this claim fails because under Georgia's “good Samaritan” provision, an undertaken duty extends only to preventing physical harm to another's person or property.¹⁸⁸ The Plaintiffs do not respond to this argument. Therefore, to the extent that the *1327 Plaintiffs assert a duty premised upon the Defendants' voluntary undertaking such a responsibility, that claim should be dismissed.

E. Negligence Per Se

[38] [39] Next, the Defendants move to dismiss the Plaintiffs' negligence per se claim.¹⁸⁹ In Count 3 of the Complaint, the Plaintiffs allege that Equifax violated Section 5 of the FTC Act, and similar state statutes, by “failing to use reasonable measures to protect Personal Information and not complying with industry standards,” and that such violation constitutes negligence per se.¹⁹⁰ “Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se.”¹⁹¹ In order to make a negligence per se claim, however, the plaintiff must show that it is within the class of persons intended to be protected by the statute and that the statute was meant to protect against the harm suffered.¹⁹²

[40] [41] The Defendants argue that the Plaintiffs fail to identify statutory text that imposes a duty with specificity upon the Defendants. Here, the Plaintiffs allege that Equifax violated Section 5 of the FTC Act. The Defendants argue that Section 5 cannot form the basis of a negligence per se claim. The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.¹⁹³ The Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect.¹⁹⁴ Additionally, one Georgia case and one case applying Georgia law both suggest that the FTC Act

can serve as the basis of a negligence per se claim.¹⁹⁵ The Defendants' motion to dismiss the negligence per se claim should be denied.

Second, the Defendants argue that *LabMD, Inc. v. Fed. Trade Comm'n*, should lead this Court to a different conclusion.¹⁹⁶ That was a direct enforcement action. There, the Eleventh Circuit noted that “standards of unfairness” must be found “in ‘clear and well-established’ policies that are expressed in the Constitution, statutes, or the common law.”¹⁹⁷ The court explained that the FTC in that case did *1328 “not explicitly cite the source of the standard of unfairness” it used in holding that LabMD's failure to implement a reasonable data security program was an unfair act or practice, but concluded that it was “apparent” that “the source is the common law of negligence.” The court then vacated the FTC's order because the order was too vague to be enforced. It did not hold that inadequate data security cannot be regulated under Section 5.

[42] [43] Next, the Defendants argue that the Plaintiffs have not sufficiently alleged injury or proximate causation. Under Georgia law, negligence per se is “not liability per se.”¹⁹⁸ Even if negligence per se is shown, a plaintiff must still prove proximate causation and actual damage to recover.¹⁹⁹ As discussed above, the Court concludes that the Plaintiffs have sufficiently alleged both a legally cognizable injury and proximate causation. Therefore, this argument is unavailing.

F. Georgia Fair Business Practices Act

Next, the Defendants move to dismiss the Plaintiffs' claims under the Georgia Fair Business Practices Act. The Georgia Fair Business Practices Act prohibits, generally, “unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce.”²⁰⁰ In Count 4 of the Complaint, the Plaintiffs allege that the Defendants violated multiple provisions of the Georgia Fair Business Practices Act, including O.C.G.A. §§ 10-1-393(a), 10-1-393(b)(5), 10-1-393(b)(7), 10-1-393(b)(9).²⁰¹ The Defendants make multiple arguments in favor of dismissal.

The Defendants first argue that the Georgia Fair Business Practices Act does not require the safeguarding of personally identifiable information.²⁰² According to the Defendants, *McConnell III* would have been decided differently if the Georgia Fair Business Practices Act contained such a

requirement.²⁰³ In *McConnell III*, the court concluded that part of the Georgia Fair Business Practices Act, O.C.G.A. § 10-1-393.8, “can not serve as the source of such a general duty to safeguard and protect the personal information of another.”²⁰⁴ That provision prohibited “intentionally communicating a person's social security number.”²⁰⁵ The court rejected the plaintiff's claim, noting that he had alleged that the defendant negligently disseminated his social security number.²⁰⁶

[44] The Plaintiffs make multiple arguments in response. However, the Court finds these arguments unpersuasive. First, they argue that *Arby's II*, decided after *McConnell III*, held that data breach victims can pursue a claim under the Georgia Fair Business Practices Act. However, that decision only considered whether the *1329 plaintiffs had adequately alleged reliance.²⁰⁷ Thus, the court's reasoning does not bear on whether *McConnell III* precluded recovery under the Georgia Fair Business Practices Act. Second, the Plaintiffs contend that *McConnell III* only stands for the proposition that the Georgia Fair Business Practices Act is not the basis of a general tort duty. However, *McConnell III*'s holding was broader than that. In *McConnell III*, the court, after examining parts of the Georgia Fair Business Practices Act, along with the Georgia Personal Identity Protection Act, concluded that there is no statutory basis for a duty to safeguard personal information in Georgia.²⁰⁸ It further explained that the Georgia legislature has not acted to establish a standard of conduct to protect the security of personal information, unlike other jurisdictions with data protection and data breach laws.²⁰⁹ Even though *McConnell III* examined the Georgia Fair Business Practices Act in the context of its provisions dealing with Social Security numbers specifically, it concluded that the entire Act, along with the rest of Georgia statutory law, did not require the safeguarding of personal information. Therefore, the Court concludes that the Georgia Fair Business Practices Act does not require businesses to safeguard personally identifiable information. This issue may be revisited depending upon the ruling of the Georgia Supreme Court in *McConnell III*.

G. Unjust Enrichment

[45] [46] The Defendants next move to dismiss the Plaintiffs' unjust enrichment claim. In Count 5 of the Complaint, the Plaintiffs allege that Equifax has been unjustly enriched by benefitting from and profiting off of the sale of the Plaintiffs' personally identifiable information, all at

the Plaintiffs' expense.²¹⁰ Unjust enrichment is an equitable doctrine that “applies when as a matter of fact there is no legal contract, but where the party sought to be charged has been conferred a benefit by the party contending an unjust enrichment which the benefitted party equitably ought to return or compensate for.”²¹¹ Thus, in order to state a claim for unjust enrichment, the Plaintiffs must show that “(1) a benefit has been conferred, (2) compensation has not been given for receipt of the benefit, and (3) the failure to so compensate would be unjust.”²¹²

The Defendants argue that, with regard to most of the Plaintiffs, personally identifiable information was conferred on Equifax by third parties, and not by the Plaintiffs themselves.²¹³ Instead, only the Contract Plaintiffs gave their information to Equifax. Thus, according to the Defendants, the unjust enrichment claims of these non-Contract Plaintiffs fail because they do not allege that they conferred anything of value on Equifax.²¹⁴

*1330 The Plaintiffs first cite *Arby's*, contending that the court in that case “sustain[ed]” the plaintiffs' claim for unjust enrichment. However, the court in *Arby's* did not consider the merits of the plaintiffs' unjust enrichment claim. Instead, it merely decided that the plaintiffs could assert a claim for unjust enrichment in the alternative to their contract claims.²¹⁵ Therefore, this case does not provide guidance as to whether the Plaintiffs have made allegations that satisfy each element of an unjust enrichment claim. The Plaintiffs also cite *Sackin v. TransPerfect Global, Inc.*²¹⁶ However, the plaintiffs in that case asserted an unjust enrichment claim under New York law, which contains different elements than such a claim under Georgia law.²¹⁷

[47] The Court concludes that the non-Contract Plaintiffs fail to establish the necessary elements of an unjust enrichment claim. The Georgia Court of Appeals has explained that “for unjust enrichment to apply, the party conferring the labor and things of value must act with the expectation that the other will be responsible for the cost. Otherwise, that party, like one who volunteers to pay the debt of another, has no right to an equitable recovery.”²¹⁸ For example, in *Sitterli v. Csachi*, the court concluded that for unjust enrichment to apply, the party conferring things of value must act with the expectation that the other will be responsible for the cost. The Plaintiffs have failed to show that they conferred a thing of value, namely their personally identifiable information, upon the Defendants

with the expectation that Equifax would be responsible for the cost. The non-Contract Plaintiffs have failed to allege that they had any such expectation.

[48] [49] [50] The Defendants also argue that the Contract Plaintiffs' unjust enrichment claims must be dismissed because those Plaintiffs have also pleaded breach of contract claims.²¹⁹ Under Georgia law, “[a] party can only recover for a claim of unjust enrichment if there is not an express contract that governs the dispute.”²²⁰ However, “[w]hile a party, indeed, cannot recover under both a breach of contract and unjust enrichment theory, a plaintiff may plead these claims in the *1331 alternative.”²²¹ Thus, the Contract Plaintiffs may assert inconsistent contract and unjust enrichment theories at this stage of the proceedings.

H. Breach of Contract

Next, the Defendants move to dismiss the Contract Plaintiffs' breach of contract claims.²²² Nineteen Plaintiffs allege that they formed a contract with Equifax, either express or implied, when they obtained credit monitoring or identity theft protection services from the company.²²³ According to these Contract Plaintiffs, Equifax's Privacy Policy constituted an agreement between Equifax and those individuals who provided personal information to it, including the Contract Plaintiffs.²²⁴ Equifax's Privacy Policy states that Equifax “restrict[s] access to personally identifiable information ... that is collected about you to only those who have a need to know that information in connection with the purpose for which it is collected and used.”²²⁵ Equifax allegedly breached this contract by failing to take steps to protect the Contract Plaintiffs' personal information.²²⁶

[51] [52] The Defendants argue that the Privacy Policy is not a contract, and even if it is, it did not impose the obligations that the Plaintiffs assert.²²⁷ They argue that the Contract Plaintiffs' purchases were governed by an express contract, with a merger clause, that does not incorporate the Privacy Policy.²²⁸ Under Georgia law, “a merger clause operates as a disclaimer of all representations not made on the face of the contract.”²²⁹ The Equifax Product Agreement and Terms of Use, which the Defendants contend was the sole contract entered into between Equifax and the Contract Plaintiffs, provides that “[t]his Agreement constitutes the entire agreement between You and Us regarding the Products and information contained on or acquired through this Site or

provided by Us.”²³⁰ However, even if this is a valid merger clause, the Equifax Terms of Use go on to provide that these terms are “[s]ubject to the conditions described on the privacy page of this Web Site.”²³¹ Therefore, the Court concludes that the merger clause in the Terms of Use does not preclude the Contract Plaintiffs’ claims.

[53] [54] The Contract Plaintiffs argue that they adequately pleaded that the Privacy Policy constituted a contract when they purchased services from Equifax, obtained their credit files, disputed their entries, or more.²³² Courts have concluded that a business’s privacy policy can constitute *1332 a stand-alone contract.²³³ However, the Contract Plaintiffs have not explicitly alleged that they read the Privacy Policy, or otherwise relied upon or were aware of the representations and assurances made in the Privacy Policy when choosing to use the Defendants’ services. Without such a showing, the Plaintiffs have failed to establish the essential element of mutual assent.²³⁴ The Plaintiffs also assert that the Product Agreement and Terms of Use incorporated the Privacy Policy.²³⁵ However, even if the Plaintiffs establish that the Privacy Policy was part of this express contract, the terms of the agreement provide that Equifax will not “be liable to any party for any direct, indirect, special or other consequential damages for any use of or reliance upon the information found at this web site.”²³⁶ Thus, even assuming the Privacy Policy was incorporated by reference, under the terms of this agreement the Plaintiffs cannot seek damages relating to the information in Equifax’s custody.²³⁷

[55] [56] [57] The Plaintiffs alternatively assert an implied contract claim.²³⁸ However, this claim fails. As discussed above, the Equifax Terms of Use contained a valid merger clause. Such a clause precludes the assertion of an implied contract claim.²³⁹ Furthermore, the Plaintiffs have failed to allege facts establishing the necessary elements of an implied contract claim. The Georgia Court of Appeals has explained that, for both express and implied contract claims, “[t]he concept of a contract requires that the minds of the parties shall meet and accord at the same time, upon the same subject matter, and in the same sense.”²⁴⁰ “In the absence of this meeting of the minds, there is no special contractual provisions between the alleged contracting parties.”²⁴¹ An implied contract only differs from an express contract in the type of proof used to prove its existence.²⁴² The same element of mutual assent is required. *1333

²⁴³ The Contract Plaintiffs allege that an implied contract was formed because “Equifax agreed to safeguard and protect the Personal Information of Plaintiffs and Class members and to timely and accurately notify them if their Personal Information was breached or compromised.”²⁴⁴ This conclusory allegation fails to establish the necessary element of mutual assent. This allegation, which contains a legal conclusion instead of a factual allegation, fails to show that the Defendants and the Contract Plaintiffs had a meeting of the minds, as required by Georgia law. Therefore, the Contract Plaintiffs’ implied contract claim fails to state a claim.

I. State Statutes

1. State Business Fraud and Consumer Protection Statutes

The Defendants move to dismiss the Plaintiffs’ claims under a variety of state business fraud and consumer protection statutes. The Defendants first argue that these statutes cannot apply to conduct that took place entirely in Georgia. Second, they contend that the Plaintiffs have not adequately alleged fraud, scienter, or injury. Third, they contend that the Plaintiffs have failed to establish that they had “consumer transactions,” as many statutes require. Fourth, the Defendants assert that the Plaintiffs fail to allege that they were under a duty to disclose. Fifth, the Defendants argue that the Plaintiffs’ claims for damages fail under statutes that provide only for equitable relief. Then, the Defendants contend that the Plaintiffs assert many claims under statutes that do not provide a private right of action. Finally, the Defendants contend that the Plaintiffs’ claims under the Georgia Uniform Deceptive Trade Practices Act must fail. The Court addresses each of these arguments in turn.

i. Extraterritoriality

[58] The Defendants contend that the deceptive trade practice laws of foreign states cannot be applied to conduct that took place in Georgia.²⁴⁵ The Defendants argue that these state statutes do not extend to conduct that occurred in Georgia. In a support of this proposition, they cite authority from eight of these states. However, that authority merely states that the statutes apply in those specific states. They do not stand for the proposition that the statutes only apply

to conduct that takes place within those states. These cases also stand for the general proposition that there are limits to the sovereignty of each state, and that there are limits to the reach of those states' laws. They do not, however, stand for the proposition that the laws of these states only extend to conduct that takes place within the states, or that the specific consumer protection statutes asserted by the Plaintiffs only extend to conduct taking place within the states. The Plaintiffs, who allege that they were harmed in each of these respective states, have adequately stated claims under these state statutes.²⁴⁶

*1334 Second, the Defendants argue that these foreign states lack authority under the Constitution to govern conduct occurring in Georgia.²⁴⁷ The Defendants cite *State Farm Mutual Automobile Insurance Company v. Campbell*.²⁴⁸ In *State Farm*, the Supreme Court imposed extraterritorial limitations on punitive damages awards.²⁴⁹ However, the Supreme Court did not hold that states are powerless to regulate out-of-state conduct. Instead, in *State Farm*, the Court held that, in the context of punitive damages, “lawful out-of-state conduct may not be used to punish a defendant” and “unlawful acts committed out of state to *other persons* may not be used to punish a defendant.”²⁵⁰ *State Farm* does not stand for the proposition that, because all of a defendant's conduct occurred outside of a state, that state cannot enforce its laws against that defendant for injuries occurring in that state.²⁵¹ The Defendants also stress that most of the Plaintiffs did not have a direct commercial relationship with Equifax, that Equifax stored its data entirely on computers located in Georgia that were serviced by employees in Georgia, and that the Defendants' acts and omissions occurred only in Georgia.²⁵² However, even assuming that this is true, the Plaintiffs have alleged that these acts that occurred in Georgia resulted in injuries in other states. These out-of-state injuries fall within the ambit of many of these foreign state statutes.²⁵³ Therefore, this argument is unavailing.

[59] The Defendants also cite *Healy v. Beer Institute, Inc.*²⁵⁴ There, the Supreme Court concluded that, under the Dormant Commerce Clause, “a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature.”²⁵⁵ However, the central point of this rule is that “a State may not adopt legislation that has the practical effect of establishing a scale of prices for use in other states.”²⁵⁶ The Court explained that “States

may not deprive businesses and consumers in other States of whatever competitive advantages they may possess based on the conditions of the local market.”²⁵⁷ Unlike the statutes at issue in *Healy* and most Dormant Commerce Clause cases, the statutes here do *1335 not involve “economic protectionism” and do not discriminate against out-of-state commerce. Thus, this limitation does not apply to the statutes here.

The Defendants then argue that, even if a harmful effect was felt outside of Georgia, that effect was the direct and proximate result of an unknown third party's act, not Equifax's act.²⁵⁸ However, as explained above, Equifax can be held liable, despite the intervening act of the criminal hackers, due to its failure to properly protect the sensitive data in Equifax's custody. Furthermore, the Defendants have not cited any authority for the proposition that they cannot be held liable under any of these state statutes due to the acts of the criminal third parties. Therefore, this argument is unpersuasive.

ii. Pleading Fraud with Particularity

[60] Next, the Defendants contend that the Plaintiffs have failed to plead fraud with particularity with regard to the state statutes.²⁵⁹ Rule 9(b) requires a complaint to “state with particularity the circumstances constituting fraud.”²⁶⁰ “A complaint satisfies Rule 9(b) if it sets forth precisely what statements or omissions were made in what documents or oral representations, who made the statements, the time and place of the statements, the content of the statements and manner in which they misled the plaintiff, and what benefit the defendant gained as a consequence of the fraud.”²⁶¹ According to the Defendants, the Plaintiffs have alleged claims under many state laws that are subject to these heightened pleading standards, including their claims for deceptive trade practices.²⁶²

[61] [62] [63] However, the Court concludes that the Plaintiffs' unfair and deceptive trade practices claims are not subject to Rule 9(b)'s heightened pleading standards. Claims are only subject to these heightened pleading standards if they “sound in fraud.”²⁶³ “A claim ‘sounds in fraud’ when a plaintiff alleges ‘a unified course of fraudulent conduct and rel[ies] entirely on that course of conduct as the basis of [that] claim.’”²⁶⁴ In *Federal Trade Commission v. Hornbeam Special Situations, LLC*, the court considered whether Rule

9(b) applied to claims under § 45(a) of the FTC Act.²⁶⁵ The court noted that, to “sound in fraud,” it is not enough that a claim be near enough to fraud, or fraud-like for Rule 9(b) to apply.²⁶⁶ In contrast, to “sound in fraud,” the elements of the claim must be similar to that of common law fraud, requiring, among other things, proof of scienter, reliance, and injury.²⁶⁷

***1336 [64]** Here, the Defendants have failed to show that the state unfair and deceptive trade practice statutes sound in fraud. They have not shown that the elements of these statutes are similar to the elements of a common law fraud, and they have not shown that the Plaintiffs' theory of recovery rests upon a unified course of fraudulent conduct. Therefore, the Court concludes that the heightened pleading standards of Rule 9(b) do not apply to these particular state statutes.

The Defendants also cite *Crespo v. Coldwell Banker Mortgage* for the proposition that the Rule 9(b) standard should be applied to claims of deceptive trade practices. However, in *Crespo*, the court applied Rule 9(b)'s heightened standards because the plaintiffs claimed that the defendant “engaged in fraud” by using deceptive trade practices.²⁶⁸ The plaintiffs asserted a fraud claim, and not a claim arising under a deceptive trade practices statute. Thus, this case is distinguishable.

iii. Scienter and Injury

[65] Then, the Defendants argue that the Plaintiffs have failed to adequately plead scienter as to their state fraud and consumer protection statutes.²⁶⁹ According to the Defendants, the Plaintiffs repeatedly assert in the Complaint that Equifax “intended to mislead” the Plaintiffs, but provide no specific factual allegations in support of this conclusion. However, the Court finds the Defendants' argument unpersuasive. The Complaint provides a number of factual allegations demonstrating Equifax's knowledge and intent with regard to its cybersecurity. For instance, the Plaintiffs allege that Equifax was aware of the importance of data security and of the previous well-publicized data breaches.²⁷⁰ It also provides allegations that, despite this knowledge of cybersecurity risks, Equifax sought to capitalize on the increased number of breaches by providing identity theft protection, instead of taking steps to improve deficiencies in its cybersecurity.²⁷¹ The Court finds that these allegations are sufficient.

[66] The Defendants also contend that the Plaintiffs have failed to adequately allege injury.²⁷² However, as explained above, the Plaintiffs have adequately alleged a legally cognizable injury. The Defendants cite one case for the proposition that “numerous” state statutes require that an injury be “ascertainable and monetary.” However, the Court concludes that the Plaintiffs have largely asserted claims that are ascertainable and monetary. The vast majority of Plaintiffs assert that they spent money taking steps to guard their identity. Furthermore, the Plaintiffs who have alleged that they were victims of identity fraud also allege injuries that are ascertainable and monetary. And, to the extent that any Plaintiffs do not plead injuries that are clearly ascertainable and monetary, the Court concludes that those claims should not be dismissed. As the Plaintiffs emphasize, this requirement comes from one District Court case in California, which has been rejected by numerous ***1337** other District Courts.²⁷³

[67] Next, the Defendants contend that the Plaintiffs' claims under state consumer protection statutes requiring “consumer transactions” fail because the non-Contract Plaintiffs do not allege that they engaged in a consumer transaction with Equifax.²⁷⁴ Although many of these state statutes provide that unfair or deceptive conduct must be done in connection with a consumer transaction, courts have interpreted these requirements liberally.²⁷⁵ Courts have concluded variously that some of these statutes do not require privity, that some of them do not require a plaintiff to be a direct purchaser of a consumer good, or that the “consumer transaction” language in some of the statutes do not actually impose a requirement for plaintiffs to meet.²⁷⁶ Therefore, the Court concludes that the state unfair and deceptive trade practices claims under statutes including “consumer transaction” language should not be dismissed.

iv. Duty to Disclose

[68] [69] Next, the Defendants contend that seventeen of the state consumer-fraud statutes do not impose liability for omissions unless there was a duty to disclose.²⁷⁷ The Court agrees. “In the absence of a confidential relationship, no duty to disclose exists when parties are engaged in arm's-length business negotiations; in fact, an arm's-length relationship by its nature excludes a confidential relationship.”²⁷⁸

The Plaintiffs contend that Equifax was under a duty to disclose due to statements it voluntarily made touting its cybersecurity.²⁷⁹ However, the vast majority of the Plaintiffs do not even allege that they were in an arms-length transaction with Equifax. Instead, most of the Plaintiffs had no relationship with Equifax. Absent such a relationship, even with these statements touting its cybersecurity, Equifax was under no general duty to disclose to the entire world.

v. Equitable Relief

[70] Next, the Defendants contend that the Plaintiffs seek money damages under four statutes that only provide for injunctive relief.²⁸⁰ According to the Defendants, the Plaintiffs cannot seek monetary damages under the Illinois, Maine, Minnesota, and Nebraska statutes. The Plaintiffs concede that they do not seek monetary damages under the Maine, Minnesota, and Nebraska Uniform Trade Secrets Acts.²⁸¹ The Plaintiffs contend, however, that violation of the Illinois Personal Information Protection Act constitutes a violation of *1338 the Illinois Consumer Fraud and Deceptive Trade Practices Act, which expressly permits damages suits.²⁸² The Court agrees. Since the Illinois Consumer Fraud and Deceptive Trade Practices Act allows for monetary damages, the Plaintiffs' claims for violation of the Personal Information Protection Act can also seek recovery of monetary damages.²⁸³

vi. Private Rights of Action

[71] [72] Finally, the Defendants contend that some of the Plaintiffs' claims arise under laws that do not provide a private right of action. Specifically, the Defendants contend that the Massachusetts Consumer Protection Act and the Nevada Deceptive Trade Practices Act do not provide for private rights of action. However, the Court finds these arguments unpersuasive. Both the Massachusetts statute²⁸⁴ and the Nevada statute²⁸⁵ are privately enforceable. Therefore, these claims should not be dismissed.

vii. Georgia Uniform Deceptive Trade Practices Act

[73] The Defendants next argue that the Plaintiffs' claims under the Georgia Uniform Deceptive Trade Practices Act,

in Count 27, must fail for the same reason that their claims under the Georgia Fair Business Practices Act also fail. The Court agrees. In *McConnell III*, the Georgia Court of Appeals concluded that there is no statutory basis under Georgia law for a duty to safeguard personal information.

2. State Data Breach Notification Statutes

Next, the Defendants move to dismiss the Plaintiffs' claims under state data breach notification statutes.²⁸⁶ The Defendants contend that twelve of the data breach statutes under which the Plaintiffs assert claims do not allow private rights of action.²⁸⁷ According to the Defendants, the data breach statutes of Colorado, Delaware, Florida, Iowa, Kansas, Maryland, Michigan, Montana, New Jersey, New York, Wisconsin, and Wyoming do not permit private actions, and the Georgia statute is silent as to whether a private right of action exists.²⁸⁸

The Plaintiffs contend that, with regard to the statutes of Iowa, Michigan, and New York, this argument ignores the statutory *1339 language.²⁸⁹ According to the Plaintiffs, courts have interpreted these statutes to be ambiguous as to this question, or that they provide non-exclusive remedies. Iowa's data-breach statute provides that “[a] violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, the attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation.”²⁹⁰ However, it further provides that “[t]he rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law.”²⁹¹ In *Target*, the court concluded that “[t]his is at least ambiguous as to whether private enforcement is permissible,” and thus the Iowa claims should not be dismissed.²⁹² The Defendants contend that this Court should not follow *Target* where its reasoning is “plainly and persuasively contradicted by other courts or the statutes themselves.”²⁹³ However, the Defendants have provided no cases contradicting this reasoning, and the *Target* holding is not inconsistent with the language of the statute. Therefore, this Court likewise concludes that the Plaintiffs' claims under the Iowa data-breach statute should not be dismissed for this reason.

[74] Similarly, Michigan's data-breach statute provides that "a person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than \$ 250.00 for each failure to provide notice" and that "[t]he attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section."²⁹⁴ However, this statute also provides that "Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law."²⁹⁵ In *Target*, the court concluded that this "implies that consumers may bring a civil action to enforce Michigan's data-breach notice statute through Michigan's consumer-protection statute or other laws," and thus this "claim will not be dismissed."²⁹⁶ Absent any compelling reasoning to the contrary provided by the Defendants, the Court agrees with the *Target* court. The Plaintiffs' claims under the Michigan data-breach statute should not be dismissed due to a lack of a private right of action.

[75] Next, New York's statute provides that "whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation."²⁹⁷ The statute also provides that "the remedies provided by this section *1340 shall be in addition to any other lawful remedy available."²⁹⁸ At first glance, these claims should survive for the same reasons the Iowa and Michigan claims survived in *Target*. However, this statute also provides that "[t]he provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section."²⁹⁹ A New York state court interpreted this provision to preclude a private action, reasoning that the "language ... militates against any implied private right of action" because it would be inconsistent with the legislative scheme.³⁰⁰ The Court agrees with this reasoning. Thus, since no private right of action exists under New York's data-breach statute, the Plaintiffs' claims under section 899-aa should be dismissed.

[76] [77] [78] The Plaintiffs then contend that four of the data-breach statutes, those of Connecticut, Maryland, Montana, and New Jersey, are enforceable through those states' consumer-protection statutes, even though the data-breach statutes themselves do not contain a private right

of action.³⁰¹ The Plaintiffs contend that violation of Connecticut's data-breach statute constitutes an unfair trade practice enforceable through its unfair trade practices statute. However, section 36a-701b explicitly states that "[f]ailure to comply with the requirements of this section shall constitute an unfair trade practices for purposes of section 42-110b and shall be enforced by the Attorney General."³⁰² The Plaintiffs, in their brief, conspicuously omit the last part of this provision, which explicitly limits enforcement to the Attorney General. Thus, the Plaintiffs' claims under section 36a-701b should be dismissed.³⁰³ Similarly, the Maryland and Montana data breach statutes are also privately enforceable through those states' unfair trade practices statutes.³⁰⁴

[79] The Court similarly concludes that New Jersey's statute provides a private right of action. New Jersey's data breach statute requires any business that conducts business in the state to "disclose any breach of security of ... 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."³⁰⁵ The language of the statute does not explicitly allow for a private right of action. The Defendants cite *Holmes v. Countrywide Financial Corp.*, where the court concluded that "[i]nsofar as the Court can tell, § 56:8-163 does not provide a private right of action for citizens to enforce its provisions."³⁰⁶ The Plaintiffs respond that violation of this notification statute is considered an unfair trade practice and thus can be privately enforced through the state's consumer protection statute.³⁰⁷ The Court agrees. Section 56:8-166 provides that violation of such a statute constitutes an unfair trade practice. Thus, this statute provides for a private right of action.

Furthermore, the data breach statutes of Colorado, Delaware, Kansas, and Wyoming contain ambiguous language as to private enforceability or provide that the statute's remedies are "non-exclusive."³⁰⁸ In *Target*, the court noted that this permissive language is "at least ambiguous as to whether there is a private right of action" and concluded that, "absent any authority construing this ambiguity to exclude private rights of action," the claims should not be dismissed.³⁰⁹ The Court finds this reasoning persuasive. The Defendants have not identified any authority construing this language as precluding private rights of action. Absent such authority, the Court declines to dismiss the Plaintiffs' claims under

the Colorado, Delaware, Kansas, and Wyoming data breach statutes.

Next, the parties disagree as to the Wisconsin data-breach statute. The Defendants contend that the statute does not permit suit by a private plaintiff, while the Plaintiffs contend that the statute is silent. The Court agrees that the statute is silent as to this question. The provision that the Defendants cite, section 134.98(4), provides that “[f]ailure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.”³¹⁰ This language does not prohibit a private action. Thus, the Court must decide whether this silence precludes, or supports, a private right of action. Neither party cites authority answering this question. The Plaintiffs cite *Target*, where the court allowed a claim under this statute to survive because neither party cited a case regarding how to interpret silence as to enforcement under Wisconsin law.³¹¹ The court concluded that, absent any such authority, the plaintiffs’ claim should survive. Likewise, the Court ***1342** here concludes that, without any authority suggesting otherwise, this claim should survive.

[80] Finally, Georgia’s statute is silent as to whether a private right of action exists.³¹² According to the Defendants, this silence means that a private right of action does not exist. The Defendants, in support of this argument, cite *State Farm Mutual Automobile Insurance Company v. Hernandez Auto Painting and Body Works, Inc.*³¹³ There, the court noted that the absence of language creating a private right of action “strongly indicates the legislature’s intention that no such cause of action be created by said statute.”³¹⁴ The Court agrees that the absence of any such language in O.C.G.A. § 10-1-912 counsels strongly against inferring a private right of action under Georgia law.³¹⁵ *Target* is not persuasive. There, the court concluded that the plaintiffs’ claims under section 10-1-912 should survive because “neither party cite[d] any case regarding how a court should interpret silence as to enforcement under Georgia law, and absent any such authority, Plaintiffs have plausibly alleged that private enforcement is possible and their Georgia claim survives.”³¹⁶ Here, the Defendants cite Georgia authority to support the proposition that such silence suggests no private right of action exists.³¹⁷ Therefore, the claims under O.C.G.A. § 10-1-912 should be dismissed.

Next, the Defendants argue that the Plaintiffs have failed to adequately allege a violation of any of the state data breach notification statutes.³¹⁸ According to the Defendants, the Complaint alleges that 41 days elapsed between Equifax’s discovery of the Data Breach and the disclosure of the incident to the public.³¹⁹ The Defendants contend these state data-breach statutes permit an entity time to determine the scope of a breach before notification, and several of the statutes even establish specific time limits. Therefore, according to the Defendants, their notification met the requirements of these statutes.

[81] However, the Court concludes that the Plaintiffs have adequately alleged a violation of many of these statutes. These statutes require notification, for example, in “the most expedient time possible and without unreasonable delay” and, for ***1343** example, within a reasonable time.³²⁰ The Plaintiffs have alleged facts from which a jury could conclude that the Defendants did not provide notice within a reasonable time, as these notification statutes require. Therefore, the Court concludes that the Plaintiffs have adequately stated a claim.

[82] The Defendants next argue that the Plaintiffs have failed to adequately allege a claim under the Maryland Social Security Number Privacy Act. This statute prohibits publicly posting or displaying an individual’s Social Security number, requiring the individual to transmit his or her Social Security number over the internet unless the connection is secure, initiating the transmission of an individual’s Social Security number over the internet unless the connection is secure, and more.³²¹ In Count 47 of the Complaint, the Plaintiffs allege that the Defendants violated the Maryland Social Security Number Privacy Act by “transmitt[ing] Plaintiff’s and Maryland Subclass members’ Social Security numbers over the Internet on unsecure connections and/or without encrypting the Social Security Numbers.”³²² According to the Defendants, these allegations fail to state a claim because they do not establish that Equifax “initiated” the transmission of any of the Plaintiffs’ Social Security numbers over the internet.³²³ The Court agrees. The Plaintiffs, analogizing their arguments under the FCRA, argue that Equifax’s conduct was so egregious that it was essentially an active participant in initiating the transmission of the Plaintiffs’ Social Security numbers. However, by suffering a criminal hack, the Defendants did not “initiate” the transmission of these Social Security numbers. While the Defendants may have been negligent, the Plaintiffs have not shown that they

“initiated the transmission” of their Social Security numbers, or engaged in any other conduct prohibit by this statute. Therefore, this claim should be dismissed.

[83] Finally, the Defendants contend that the Plaintiffs have failed to allege any injury resulting from a delay in notification.³²⁴ According to the Defendants, the Plaintiffs have not alleged when any injury occurred, and thus have not alleged any damage occurring between the time that Equifax should have notified them of the Data Breach, and the time that Equifax did publicly disclose the Data Breach.³²⁵ However, the *Target* court rejected this exact argument. There, the court reasoned that such an argument is premature at this stage and that plaintiffs need only plead “a ‘short and plain statement’ of their claims” under Rule 8.³²⁶ The Plaintiffs note that they could have frozen their credit earlier, or taken other precautions.³²⁷ At this stage of the litigation, such allegations are sufficient.

3. “Non-Existent” Plaintiffs

[84] Next, the Defendants contend that the Plaintiffs' claims under the laws of *1344 Puerto Rico and the Virgin Islands must be dismissed because no Plaintiff has alleged any connection to, or residence in, either of these territories.³²⁸ However, the Court concludes that the Plaintiffs have adequately alleged claims under Puerto Rico and Virgin Islands law. At this stage of the litigation, it is sufficient to allege that individuals nationwide, including individuals in Puerto Rico and the Virgin Islands, suffered injury from the Data Breach. In *Target*, the court came to the same conclusion, noting that the plaintiffs only need to plausibly allege “that they have standing to represent a class of individuals in every state and the District of Columbia, and thus that they have standing to raise state-law claims in those jurisdictions.”³²⁹ The court explained that:

As Target undoubtedly knows, there are consumers in Delaware, Maine, Rhode Island, Wyoming, and the District of Columbia whose personal financial information was stolen in the 2013 breach. To force Plaintiffs' attorneys to search out those individuals at this stage serves no

useful purpose. In this case, and under the specific facts presented here, the Article III standing analysis is best left to after the class-certification stage. Should a class be certified, and should that class as certified contain no members from certain states, Target may renew its arguments regarding standing.³³⁰

Likewise, the Plaintiffs have alleged, and it is very likely, that there are consumers in Puerto Rico and the Virgin Islands whose personal information was compromised in the Data Breach. *Griffin v. Dugger*, cited by the Defendants, is distinguishable because that decision was made in the context of class certification, where such questions are most appropriate.³³¹ Thus, at this stage, the Plaintiffs have adequately alleged a claim under the laws of these territories.³³²

4. O.C.G.A. § 13-6-11

Finally, the Defendants move to dismiss the Consumer Plaintiffs' claims under O.C.G.A. § 13-6-11. This statute provides that:

The expenses of litigation generally shall not be allowed as a part of the damages; but where the plaintiff has specially pleaded and has made prayer therefor and where the defendant has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense, the jury may allow them.³³³

The Consumer Plaintiffs contend that they are entitled to recovery under section 13-6-11 because they have plausibly alleged that “Equifax's conduct leading up to the breach was egregious and that both the *1345 breach and injury were foreseeable.”³³⁴ The Defendants argue that this claim should be dismissed because there is a bona fide controversy or

dispute between the parties, and because the Plaintiffs have pleaded no facts suggesting bad faith.³³⁵

[85] [86] [87] The Plaintiffs do not appear to seek attorneys' fees based upon stubborn litigiousness or unnecessary trouble or extent. Thus, the basis for their claim must be under the "bad faith prong" of [section 13-6-11](#).³³⁶ " 'Bad faith' is 'bad faith connected with the transaction and dealings out of which the cause of action arose, rather than bad faith in defending or resisting the claim after the cause of action has already arisen.' " ³³⁷ "Bad faith requires more than 'bad judgment' or 'negligence,' rather the statute imports a 'dishonest purpose' or some 'moral obliquity' and implies 'conscious doing of wrong' and a 'breach of known duty through some motive of interest of ill will.' " The Court concludes that the Plaintiffs have alleged facts supporting bad faith. In the Complaint, the Plaintiffs have alleged that the Defendants knew of severe deficiencies in

their cybersecurity, and of serious threats, but nonetheless declined to act. Based upon Georgia caselaw, the Court concludes that these allegations are sufficient for a claim of bad faith under [section 13-6-11](#).

IV. Conclusion

For the reasons stated above, the Defendants' Motion to Dismiss the Consolidated Consumer Class Action Complaint [Doc. 425] is GRANTED in part and DENIED in part.

SO ORDERED, this 28 day of January, 2019.

All Citations

362 F.Supp.3d 1295

Footnotes

1 Consolidated Consumer Class Action Compl. ¶ 2 [Doc. 374].

2 *Id.*

3 *Id.* ¶ 2.

4 *Id.* ¶ 4.

5 *Id.*

6 *Id.*

7 *Id.* ¶ 109.

8 *Id.*

9 *Id.* ¶¶ 110-11.

10 *Id.* ¶ 112.

11 *Id.* ¶ 11.

12 *Id.*

13 *Id.* ¶ 134.

14 *Id.*

15 *Id.* ¶ 135.

16 *Id.* ¶ 137.

17 *Id.* ¶ 144.

18 *Id.* ¶¶ 146, 159-65.

19 *Id.* ¶ 147.

20 *Id.* ¶ 146.

21 *Id.* ¶¶ 166-82.

22 *Id.* ¶¶ 177-82.

23 *Id.* ¶ 178.

24 *Id.* ¶ 216.

25 *Id.* ¶¶ 183-86.

26 *Id.* ¶ 184.

27 *Id.* ¶ 187.

28 *Id.* ¶ 188.

- 29 *Id.* ¶ 189.
- 30 *Id.* ¶ 195.
- 31 *Id.*
- 32 *Id.* ¶ 195.
- 33 *Id.* ¶ 11.
- 34 *Id.* ¶¶ 196-97.
- 35 *Id.* ¶ 197.
- 36 *Id.* ¶ 198.
- 37 *Id.* ¶ 201.
- 38 *Id.*
- 39 *Id.* ¶ 227.
- 40 *Id.* ¶¶ 214-226.
- 41 *Ashcroft v. Iqbal*, 556 U.S. 662, 129 S.Ct. 1937, 1949, 173 L.Ed.2d 868 (2009); FED. R. CIV. P. 12(b)(6).
- 42 *Bell Atlantic v. Twombly*, 550 U.S. 544, 556, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007).
- 43 See *Quality Foods de Centro America, S.A. v. Latin American Agribusiness Dev. Corp., S.A.*, 711 F.2d 989, 994-95 (11th Cir. 1983); see also *Sanjuan v. American Bd. of Psychiatry and Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff “receives the benefit of imagination”).
- 44 See *Lombard's, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985), *cert. denied*, 474 U.S. 1082, 106 S.Ct. 851, 88 L.Ed.2d 892 (1986).
- 45 *Frank Briscoe Co., Inc. v. Ga. Sprinkler Co., Inc.*, 713 F.2d 1500, 1503 (11th Cir.1983) (“A federal court faced with the choice of law issue must look for its resolution to the choice of law rules of the forum state.”).
- 46 *Dowis v. Mud Slingers, Inc.*, 279 Ga. 808, 816, 621 S.E.2d 413 (2005); *Int'l Bus. Machines Corp. v. Kemp*, 244 Ga. App. 638, 640, 536 S.E.2d 303 (2000).
- 47 *Mullins v. M.G.D. Graphics Sys. Grp.*, 867 F.Supp. 1578, 1581 (N.D. Ga. 1994).
- 48 *In re Tri-State Crematory Litig.*, 215 F.R.D. 660, 677 (N.D. Ga. 2003) (internal quotations omitted). The Georgia Supreme Court has recently reaffirmed this exception. See *Coon v. The Med. Ctr., Inc.*, 300 Ga. 722, 729, 797 S.E.2d 828 (2017) (“In the absence of a statute, however, at least with respect to a state where the common law is in force, a Georgia court will apply the common law as expounded by the courts of Georgia.”).
- 49 The Plaintiffs argue that Georgia law should apply unless the Court decides “that Georgia law is adverse to the common law claims of the national class pled in the Complaint, in which case it will be necessary to consider the common law of each state applicable to the proposed alternative, state-specific classes.” Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 9. However, the Plaintiffs cite no authority for such a proposition. The Court concludes that Georgia law will govern this case.
- 50 15 U.S.C. § 1681b(a).
- 51 Consolidated Consumer Class Action Compl. ¶¶ 321, 324.
- 52 Defs.' Mot. to Dismiss, at 12-15.
- 53 *Id.* at 15-16.
- 54 15 U.S.C. § 1681b(a).
- 55 *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595, at *2 (C.D. Cal. Dec. 29, 2016) (quoting *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *3 (N.D. Ill. Jan. 21, 2015)).
- 56 *Id.*
- 57 See, e.g., *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118, 2017 WL 4987663, at *4 (S.D. Ohio Aug. 16, 2017).
- 58 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 46-47.
- 59 Defs.' Mot. to Dismiss, at 13-15.
- 60 15 U.S.C. § 1681b.
- 61 15 U.S.C. § 1681a(d)(1).
- 62 See, e.g., *Parker v. Equifax Info. Servs., LLC*, No. 2:15-cv-14365, 2017 WL 4003437, at *3 (E.D. Mich. Sept. 12, 2017).
- 63 *Id.* (“The accumulation of biographical information from Equifax's products does not constitute a consumer report because the information does not bear on Parker's credit worthiness.”).
- 64 *Id.* at *1, *3.
- 65 15 U.S.C. § 1681e.

- 66 [Experian](#), 2016 WL 7973595, at *2 (quoting [Moreland v. CoreLogic SafeRent LLC](#), No. SACV 13-470 AG, 2013 WL 5811357, at *6 (C.D. Cal. Oct. 25, 2013)).
- 67 Consolidated Consumer Class Action Compl. ¶¶ 417-27.
- 68 *Id.* ¶¶ 418-20.
- 69 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 50-51.
- 70 Defs.' Mot. to Dismiss, at 16. Importantly, the Defendants do not seem to contend that the Plaintiffs have failed to establish standing. Instead, the Defendants contend that the Plaintiffs have not established a legally cognizable harm, or proximate causation, as elements of a tort claim. The Plaintiffs highlight this distinction in their brief. See Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 19 ("Equifax does not dispute standing and instead argues that Plaintiffs fail to plead 'legally cognizable harms' under Georgia law."). The Defendants do not disagree.
- 71 *Id.*
- 72 *Id.*
- 73 [Whitehead v. Cuffie](#), 185 Ga. App. 351, 353, 364 S.E.2d 87 (1987).
- 74 *Id.*
- 75 Defs. Mot. to Dismiss, at 17.
- 76 See Consolidated Consumer Class Action Compl. ¶¶ 13-108.
- 77 See, e.g., [In re Arby's Restaurant Grp. Inc. Litig.](#), No. 1:17-cv-0514-AT, 2018 WL 2128441, at *11 (N.D. Ga. Mar. 5, 2018).
- 78 Defs.' Mot. to Dismiss, at 17.
- 79 See [Rite Aid of Ga, Inc. v. Peacock](#), 315 Ga. App. 573, 580, 726 S.E.2d 577 (2012).
- 80 *Id.* at 573, 726 S.E.2d 577.
- 81 *Id.* at 574, 726 S.E.2d 577.
- 82 *Id.* at 576, 726 S.E.2d 577.
- 83 See, e.g., [Resnick v. AvMed, Inc.](#), 693 F.3d 1317, 1323 (11th Cir. 2012); [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); [In re Arby's Rest. Grp. Inc. Litig.](#), 317 F.Supp.3d 1222 (N.D. Ga. 2018).
- 84 Defs.' Mot. to Dismiss, at 17.
- 85 [Finnerty v. State Bank & Trust Co.](#), 301 Ga. App. 569, 687 S.E.2d 842 (2009), *disapproved of in part on other grounds by Cumberland Contractors, Inc. v. State Bank & Trust Co.*, 327 Ga. App. 121, 126 n.4, 755 S.E.2d 511 (2014).
- 86 *Id.* at 571, 687 S.E.2d 842.
- 87 *Id.* at 571-72, 687 S.E.2d 842.
- 88 *Id.*
- 89 Defs.' Mot. to Dismiss, at 18.
- 90 [Randolph v. ING Life Ins. & Annuity Co.](#), 973 A.2d 702, 704 (D.C. 2009).
- 91 Defs.' Reply Br., at 9.
- 92 [Collins v. Athens Orthopedic Clinic](#), 347 Ga. App. 13, 815 S.E.2d 639 (2018).
- 93 *Id.* at 18, 815 S.E.2d 639.
- 94 *Id.*
- 95 Defs.' Reply Br., at 9.
- 96 [Collins](#), 347 Ga. App. at 18, 815 S.E.2d 639.
- 97 Defs.' Mot. to Dismiss, at 19-20.
- 98 Consolidated Consumer Class Action Compl. ¶¶ 26, 33, 60.
- 99 Defs.' Mot. to Dismiss, at 19.
- 100 [Resnick v. AvMed, Inc.](#), 693 F.3d 1317, 1324 (11th Cir. 2012) (explaining that, under notice pleading standards, plaintiffs need not allege that they experienced "unreimbursed losses" as a result of payment card fraud).
- 101 Defs.' Mot. to Dismiss, at 20-21.
- 102 [Anderson v. Barrow Cty.](#), 256 Ga. App. 160, 163, 568 S.E.2d 68 (2002).
- 103 *Id.*
- 104 [Grinold v. Farist](#), 284 Ga. App. 120, 121, 643 S.E.2d 253 (2007) (quoting [Feazell v. Gregg](#), 270 Ga. App. 651, 655, 607 S.E.2d 253 (2004)).
- 105 *Id.* at 121-22, 643 S.E.2d 253.

- 106 Defs.' Mot. to Dismiss, at 21.
- 107 *Id.*
- 108 See, e.g., Consolidated Consumer Class Action Compl. ¶ 17 (“As a result of the breach, Plaintiff Sanchez has suffered identity theft in the form of an unauthorized credit card opened in his name using his Personal Information.”).
- 109 *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *19 (N.D. Cal. Aug. 30, 2017) (quoting *In re Anthem, Inc. Data Breach Litig.*, 162 F.Supp.3d 953, 988 (N.D. Cal. 2016)).
- 110 See, e.g., Consolidated Consumer Class Action Compl. ¶ 15 (“[A]s a result of the breach, Plaintiff Bishop paid to maintain his credit monitoring services from TransUnion and Experian in order to mitigate possible harm and spent time and effort monitoring his accounts for fraudulent activity.”).
- 111 The Court also declines to consider the Defendants' argument that over 1,500 data breaches occurred in 2017. Even if this is true, this assertion has no basis in the allegations of the Complaint, and should not be considered at this stage of the litigation.
- 112 Defs.' Mot. to Dismiss, at 21-22.
- 113 *Id.* at 22.
- 114 *In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *3 (N.D. Ga. Mar. 5, 2018) (quoting *Bradley Center, Inc. v. Wessner*, 250 Ga. 199, 201, 296 S.E.2d 693 (1982)).
- 115 *Goldstein, Garber, & Salama, LLC v. J.B.*, 300 Ga. 840, 841, 797 S.E.2d 87 (2017) (quoting *Ontario Sewing Mach. Co., Ltd. v. Smith*, 275 Ga. 683, 686, 572 S.E.2d 533 (2002)).
- 116 *Id.* (quoting *Ontario Sewing Mach.*, 275 Ga. at 686, 572 S.E.2d 533).
- 117 *Id.* at 842, 797 S.E.2d 87 (internal quotations omitted).
- 118 *Arby's*, 2018 WL 2128441, at *4 (quoting *Sturbridge Partners, Ltd. v. Walker*, 267 Ga. 785, 786, 482 S.E.2d 339 (1997)).
- 119 *Id.* (quoting *Sturbridge Partners, Ltd.*, 267 Ga. at 786, 482 S.E.2d 339).
- 120 *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).
- 121 *Arby's*, 2018 WL 2128441, at *5.
- 122 *Id.* at *5-6.
- 123 *Id.* at *4 (internal quotations omitted).
- 124 Consolidated Consumer Class Action Compl. ¶¶ 159-65.
- 125 *Id.* at ¶¶ 166-82.
- 126 *Id.* ¶ 179.
- 127 Defs.' Mot. to Dismiss, at 22-23.
- 128 Consolidated Consumer Class Action Compl. ¶ 146.
- 129 See, e.g., *id.* ¶¶ 159-65.
- 130 *Id.* ¶¶ 160-65.
- 131 Defs.' Mot. to Dismiss, at 23.
- 132 *General Elec. Co. v. Lowe's Home Centers, Inc.*, 279 Ga. 77, 78, 608 S.E.2d 636 (2005).
- 133 *Hanover Ins. Co. v. Hermosa Const. Grp., LLC*, 57 F.Supp.3d 1389, 1395 (N.D. Ga. 2014).
- 134 *Liberty Mut. Fire Ins. Co. v. Cagle's, Inc.*, No. 1:10-cv-2158-TWT, 2010 WL 5288673, at *3 (N.D. Ga. Dec. 16, 2010).
- 135 *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F.Supp.3d 1359, 1365 (S.D. Fla. 2017).
- 136 Defs.' Mot. to Dismiss, at 24.
- 137 Consolidated Consumer Class Action Compl. ¶ 334.
- 138 *Id.* ¶¶ 337, 340.
- 139 This argument seems more than a little cynical in light of Equifax's public description of itself as the “trusted steward” of consumer data.
- 140 *Dupree v. Keller Indus., Inc.*, 199 Ga. App. 138, 141, 404 S.E.2d 291 (1991) (internal quotations omitted).
- 141 *Access Mgmt. Grp., L.P. v. Hanham*, 345 Ga. App. 130, 133, 812 S.E.2d 509 (2018) (internal quotations omitted).
- 142 *Id.* (internal quotations omitted).
- 143 *Bradley Center, Inc. v. Wessner*, 250 Ga. 199, 201, 296 S.E.2d 693 (1982).
- 144 Defs.' Mot. to Dismiss, at 24.
- 145 *Id.*
- 146 *McConnell v. Dep't of Labor (McConnell III)*, 345 Ga. App. 669, 670, 814 S.E.2d 790 (2018).

- 147 *Id.*
- 148 *Id.*
- 149 *McConnell v. Dep't of Labor (McConnell I)*, 337 Ga. App. 457, 462, 787 S.E.2d 794 (2016).
- 150 *Id.* at 460, 787 S.E.2d 794.
- 151 *Id.* at 461-62, 787 S.E.2d 794.
- 152 *Id.* at 462, 787 S.E.2d 794.
- 153 *Id.* at 460 n.4, 787 S.E.2d 794.
- 154 *McConnell v. Dep't of Labor (McConnell II)*, 302 Ga. 18, 18-19, 805 S.E.2d 79 (2017).
- 155 *McConnell v. Dep't of Labor (McConnell III)*, 345 Ga. App. 669, 678-679, 814 S.E.2d 790 (2018).
- 156 *Id.* at 676-79, 814 S.E.2d 790.
- 157 *Id.* at 679, 814 S.E.2d 790.
- 158 Defs.' Mot. to Dismiss, at 26.
- 159 See 15 U. S. C. § 1681b(a).
- 160 Federal Trade Commission Act. 15 U.S.C.A. § 45(a); *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015).
- 161 See 15 U.S.C. § 6801(b).
- 162 See 16 C.F.R. § 314.4(b-e).
- 163 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 9.
- 164 *In re The Home Depot, Inc. Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *1 (N.D. Ga. May 18, 2016).
- 165 *Id.* at *3.
- 166 *Id.* (quoting *Bradley Ctr., Inc. v. Wessner*, 250 Ga. 199, 201, 296 S.E.2d 693 (1982)).
- 167 *Id.* at *4.
- 168 *In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-1035-AT, 2018 WL 2128441, at *5 (N.D. Ga. Mar. 5, 2018).
- 169 *Id.* at *5.
- 170 *Id.* at *6.
- 171 *Id.* at *7.
- 172 Defs.' Mot. to Dismiss, at 29-30.
- 173 *Id.*
- 174 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 14-15.
- 175 *Id.* at 14-15.
- 176 *Id.* at 16.
- 177 *McConnell I*, 337 Ga. App. at 461 n.4, 787 S.E.2d 794.
- 178 *Id.*
- 179 See *Home Depot*, 2016 WL 2897520, at *4.
- 180 *Bradley Ctr., Inc. v. Wessner*, 250 Ga. 199, 199-200, 296 S.E.2d 693 (1982).
- 181 *Id.* at 200, 296 S.E.2d 693.
- 182 *Id.* at 200-02, 296 S.E.2d 693.
- 183 *Id.* at 201, 296 S.E.2d 693.
- 184 *Id.* at 202, 296 S.E.2d 693.
- 185 See *Underwood v. Select Tire, Inc.*, 296 Ga. App. 805, 809, 676 S.E.2d 262 (2009) (describing the general duty one owes to the world to not subject them to an unreasonable risk of harm).
- 186 Defs.' Mot. to Dismiss, at 32.
- 187 Consolidated Consumer Class Action Comp. ¶ 338.
- 188 Defs.' Mot. to Dismiss, at 32.
- 189 Defs.' Mot. to Dismiss, at 34.
- 190 Consolidated Consumer Class Action Compl. ¶¶ 350-51.
- 191 *Pulte Home v. Simerly*, 322 Ga. App. 699, 705, 746 S.E.2d 173 (2013).
- 192 *Amick v. BM & KM, Inc.*, 275 F.Supp.2d 1378, 1382 (N.D. Ga. 2003).
- 193 15 U.S.C.A. § 45(a); *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015).

- 194 See *Arby's*, 2018 WL 2128441, at *8 (concluding that similar allegations were sufficient to plead a violation of Section 5).
- 195 *Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360-JCT, 2014 WL 637762, at *13-14 (W.D. Va. Feb. 12, 2014) (applying Georgia law); *Legacy Acad., Inc. v. Mamilove, LLC*, 328 Ga. App. 775, 790, 761 S.E.2d 880 (2014), *aff'd in part and rev'd in part on other grounds*, 297 Ga. 15, 771 S.E.2d 868 (2015).
- 196 *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018).
- 197 *Id.* at 1231.
- 198 *Hite v. Anderson*, 284 Ga. App. 156, 158, 643 S.E.2d 550 (2007).
- 199 *Id.*
- 200 O.C.G.A. § 10-1-393(a).
- 201 Consolidated Consumer Class Action Compl. ¶¶ 355-80.
- 202 Defs.' Mot. to Dismiss, at 38-39.
- 203 *Id.* at 38.
- 204 *McConnell v. Dep't of Labor (McConnell III)*, 345 Ga. App. 669, 678, 814 S.E.2d 790 (2018).
- 205 *Id.* (emphasis omitted).
- 206 *Id.*
- 207 See *In re Arby's Restaurant Grp. Inc. Litig.*, 317 F.Supp.3d 1222, 1224 (N.D. Ga. 2018).
- 208 *McConnell III*, 345 Ga. App. 669, 677-79, 814 S.E.2d 790.
- 209 *Id.* at 679, 814 S.E.2d 790.
- 210 Consolidated Consumer Class Action Compl. ¶¶ 382-91.
- 211 *Engram v. Engram*, 265 Ga. 804, 806, 463 S.E.2d 12 (1995) (quotations and some punctuation omitted).
- 212 *Hill v. Clark*, No. 2:11-CV-0057-RWS, 2012 WL 787398, at *6 (N.D. Ga. Mar. 7, 2012).
- 213 Defs.' Mot. to Dismiss, at 42.
- 214 *Id.*
- 215 See *In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *17 (N.D. Ga. Mar. 5, 2018) ("Therefore, the Consumer Plaintiffs are entitled to assert a claim for unjust enrichment in the alternative to their claim for breach of an implied-in-fact contract.").
- 216 *Sackin v. TransPerfect Global, Inc.*, 278 F.Supp.3d 739 (S.D.N.Y. 2017).
- 217 See *id.* at 751 (quoting *Ga. Malone & Co. v. Rieder*, 19 N.Y.3d 511, 950 N.Y.S.2d 333, 973 N.E.2d 743 (2012)) (The plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered.); see also *Engram v. Engram*, 265 Ga. 804, 806, 463 S.E.2d 12 (1995) ("[T]he undisputed evidence shows that the parties never intended that appellees be responsible for the cost of the bedroom addition.").
- 218 *Sitterli v. Csachi*, 344 Ga. App. 671, 673, 811 S.E.2d 454 (2018) (internal quotations and alterations omitted).
- 219 Defs.' Mot. to Dismiss, at 42.
- 220 *Arby's*, 2018 WL 2128441, at *17 (citing *Fed. Ins. Co. v. Westside Supply Co.*, 264 Ga. App. 240, 248, 590 S.E.2d 224 (2003)).
- 221 *Clark v. Aaron's, Inc.*, 914 F.Supp.2d 1301, 1309 (N.D. Ga. 2012).
- 222 Defs.' Mot. to Dismiss, at 44-49.
- 223 Consolidated Consumer Class Action Compl. ¶¶ 405, 410.
- 224 *Id.* ¶ 401.
- 225 *Id.* ¶ 152.
- 226 *Id.* ¶ 407.
- 227 Defs.' Mot. to Dismiss, at 44.
- 228 *Id.*
- 229 *Ekeledo v. Amporful*, 281 Ga. 817, 819, 642 S.E.2d 20 (2007).
- 230 See [Doc. 464-1], at 7.
- 231 *Id.* at 8.
- 232 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 40-41.
- 233 See, e.g., *In re JetBlue Airways Corp. Privacy Lit.*, 379 F.Supp.2d 299, 325 (E.D.N.Y. 2005) ("Although plaintiffs do allege that the privacy policy constituted a term in the contract of carriage, they argue alternatively that a stand-alone contract

- was formed at the moment they made flight reservations in reliance on express promises contained in JetBlue's privacy policy. JetBlue posits no persuasive argument why this alternative formulation does not form the basis of a contract.”).
- 234 See, e.g., *id.* at 325 (“JetBlue further argues that failure to allege that plaintiffs read the privacy policy defeats any claim of reliance. Although plaintiffs do not explicitly allege that the class members actually read or saw the privacy policy, they do allege that they and other class members relied on the representations and assurances contained in the privacy policy when choosing to purchase air transportation from JetBlue.”).
- 235 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 41-42.
- 236 See [Doc. 464-1], at 7.
- 237 Due to the existence of a merger clause, the Contract Plaintiffs' implied contract claims also must necessarily fail.
- 238 Consolidated Consumer Class Action Compl. ¶¶ 409-16.
- 239 See *Ekeledo v. Amporful*, 281 Ga. 817, 819, 642 S.E.2d 20 (2007) (“In essence, a merger clause operates as a disclaimer of all representations not made on the face of the contract.”).
- 240 *Donaldson v. Olympic Health Spa, Inc.*, 175 Ga. App. 258, 259, 333 S.E.2d 98 (1985).
- 241 *Id.*
- 242 *Grange Mut. Cas. Co. v. Woodard*, 300 Ga. 848, 853, 797 S.E.2d 814 (2017).
- 243 *Id.*
- 244 Consolidated Consumer Class Action Compl. ¶ 411.
- 245 Defs.' Mot. to Dismiss, at 53-54.
- 246 See, e.g., *McKinnon v. Dollar Thrifty Auto. Grp., Inc.*, No. 12-4457 SC, 2013 WL 791457, at *5 (N.D. Cal. Mar. 4, 2013) (“California residents can bring claims against out-of-state defendants if their injuries occurred in California.”).
- 247 Defs.' Mot. to Dismiss, at 54.
- 248 *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 123 S.Ct. 1513, 155 L.Ed.2d 585 (2003).
- 249 *Id.* at 421-22, 123 S.Ct. 1513.
- 250 *Crouch v. Teledyne Cont'l Motors, Inc.*, No. 10-00072-KD-N, 2011 WL 1539854, at *4 (S.D. Ala. April 21, 2011).
- 251 *Id.* (“Neither *State Farm* nor *Sand Hill [Energy, Inc. v. Smith]*, 142 S.W.3d 153 (Ky.2004)] supports TCM's conclusion that because all of its ‘conduct’ occurred outside of Kentucky, punitive damages may not be awarded against it.”).
- 252 Defs.' Mot. to Dismiss, at 55.
- 253 See *Hendricks v. Ford Motor Co.*, No. 4:12CV71, 2012 WL 4478308, at *4 (E.D. Tex. Sept. 27, 2012) (“In *Campbell*, however, fundamental to the Supreme Court's decision was that fact that the out-of-state conduct bore no relation to the plaintiff's harm.”).
- 254 *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 109 S.Ct. 2491, 105 L.Ed.2d 275 (1989).
- 255 *Id.* at 336, 109 S.Ct. 2491.
- 256 *Id.* (internal quotations omitted).
- 257 *Id.* at 339, 109 S.Ct. 2491 (internal quotations omitted).
- 258 Defs.' Mot. to Dismiss, at 55.
- 259 *Id.* at 56-59.
- 260 FED. R. CIV. P. 9(b).
- 261 *In re Theragenics Corp. Sec. Litig.*, 105 F.Supp.2d 1342, 1348 (N.D. Ga. 2000) (citing *Brooks v. Blue Cross and Blue Shield of Fla., Inc.*, 116 F.3d 1364, 1371 (11th Cir. 1997)).
- 262 Defs.' Mot. to Dismiss, at 56-57.
- 263 See *In re AFC Enters., Inc. Sec. Litig.*, 348 F.Supp.2d 1363, 1376 (N.D. Ga. 2004).
- 264 *Burgess v. Religious Tech. Ctr., Inc.*, CIV.A. No. 1:13-cv-02217-SCJ, 2014 WL 11281382, at *6 (N.D. Ga. Feb. 19, 2014).
- 265 *Fed. Trade Comm'n v. Hornbeam Special Situations, LLC*, 308 F.Supp.3d 1280, 1286-87 (N.D. Ga. 2018).
- 266 *Id.* at 1287.
- 267 *Id.*
- 268 *Crespo v. Coldwell Banker Mortg.*, 599 F. App'x 868, 873 (11th Cir. 2014).
- 269 Defs.' Mot. to Dismiss, at 59-60.
- 270 Consolidated Consumer Class Action Compl. ¶ 159.
- 271 *Id.* ¶¶ 146-49.
- 272 Defs.' Mot. to Dismiss, at 60.

- 273 See, e.g., *Corona v. Sony Pictures Entertainment, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *3-4 (C.D. Cal. June 15, 2015).
- 274 Defs.' Mot. to Dismiss, at 61-62.
- 275 See Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, Ex. B [Doc. 452-2].
- 276 *Id.*
- 277 Defs.' Mot. to Dismiss, at 63.
- 278 *Infrasource, Inc. v. Hahn Yalena Corp.*, 272 Ga. App. 703, 705, 613 S.E.2d 144 (2005).
- 279 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 58-59.
- 280 Defs.' Mot. to Dismiss, at 63.
- 281 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 60. They note that they seek all relief allowed by law, including attorneys' fees, which are available under each statute. *Id.*
- 282 *Id.*
- 283 See 815 ILCS § 505-10a(a). In *Allen v. Woodfield Chevrolet, Inc.*, the Supreme Court of Illinois declared amendments to this statute unconstitutional under the Illinois Constitution. See *Allen v. Woodfield Chevrolet, Inc.*, 208 Ill.2d 12, 280 Ill.Dec. 501, 802 N.E.2d 752, 764-65 (2003). These amendments "changed the substantive and procedural requirements for consumer fraud claims against a single group of defendants, namely, new and used vehicle dealers." *Id.*, 280 Ill.Dec. 501, 802 N.E.2d at 756. The court concluded that these amendments violated the Illinois Constitution's prohibition against special legislation. *Id.*, 280 Ill.Dec. 501, 802 N.E.2d at 759-760. However, it noted that its decision left intact the rights provided for by the statute prior to this legislation, including a private right of action. See *id.*, 280 Ill.Dec. 501, 802 N.E.2d at 765 ("The effect of our determination is to relegate the parties to such rights as they may have had prior to the enactment of this legislation.").
- 284 See *In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009).
- 285 See N.R.S. § 41.600(1).
- 286 Defs.' Mot. to Dismiss, at 65.
- 287 Defs.' Mot. to Dismiss, at 65.
- 288 *Id.*
- 289 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 62.
- 290 IOWA CODE § 715C.2(9)(a).
- 291 *Id.* § 715C.2(9)(b).
- 292 *In re Target Corp. Data Sec. Breach Litig.*, 66 F.Supp.3d 1154, 1169 (D. Minn. 2014).
- 293 Defs.' Reply Br., at 34.
- 294 Mich. Comp. Laws § 445.72(13).
- 295 *Id.* § 445.72(15).
- 296 *Target*, 66 F.Supp.3d at 1169.
- 297 N.Y. GEN. BUS. LAW § 899-aa(6)(a).
- 298 *Id.* § 899-aa(6)(b).
- 299 *Id.* § 899-aa(9).
- 300 See *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 49 Misc.3d 1027, 19 N.Y.S.3d 850, 858 (N.Y. Sup. Ct. 2015).
- 301 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 63.
- 302 CONN. GEN. STAT. § 36a-701b(g) (emphasis added).
- 303 See *Target*, 66 F.Supp.3d at 1168 (concluding that the language of § 36a-701b(g) "clearly limits enforcement power to the state's attorney general").
- 304 See MD. CODE ANN. COM. LAW § 14-3508 (noting that a violation of the Maryland Personal Information Protection Act constitutes "an unfair or deceptive trade practice within the meaning of Title 13 of this article"); Mont. Code Ann. § 30-14-1705(3) (providing that "[a] violation of this part is a violation of 30-14-103"); *id.* § 30-14-133(1) (providing that a consumer suffering a loss under § 30-14-103 may bring an individual action).
- 305 See N.J. STAT. ANN. § 56:8-163.
- 306 *Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205, 2012 WL 2873892, at *13 (W.D. Ky. July 12, 2012).
- 307 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 63.
- 308 See COLO. REV. STAT. § 6-1-716(4) (providing that "[t]he attorney general may bring an action in law or equity to address violations of this section" and that "[t]he provisions of this section are not exclusive"); DEL. CODE ANN. tit. 6 § 12B-104(a)

(providing that “the Attorney General may bring an action in law or equity to address the violations of this chapter” and that “[t]he provisions of this chapter are not exclusive”); [KAN. STAT. ANN. § 50-7a02\(g\)](#) (providing that “the attorney general is empowered to bring an action in law or equity to address violations of this section” and that “[t]he provisions of this section are not exclusive”); [Wyo. Stat. Ann. § 40-12-502\(f\)](#) (providing that “[t]he attorney general may bring an action in law or equity to address any violation of this section” and that “[t]he provisions of this section are not exclusive”).

309 See [Target](#), 66 F.Supp.3d at 1169.

310 [WIS. STAT. § 134.98\(4\)](#).

311 [Target](#), 66 F.Supp.3d at 1170. In [Target](#), the court noted that Wisconsin’s statute, like Georgia’s, is silent on enforcement, and that it should not be dismissed.

312 See [O.C.G.A. § 10-1-912](#).

313 Defs.’ Mot. to Dismiss, at 65.

314 [State Farm Mut. Auto. Ins. Co. v. Hernandez Auto Painting & Body Works, Inc.](#), 312 Ga. App. 756, 761, 719 S.E.2d 597 (2011) (internal quotations omitted).

315 See *id.*; see also [Cross v. Tokio Marine & Fire Ins. Co. Ltd.](#), 254 Ga. App. 739, 741, 563 S.E.2d 437 (2002) (“[T]he absence of language in [OCGA § 33-3-28](#) creating a private right of action ‘strongly indicates the legislature’s intention that no such cause of action be created by said statute.’”).

316 [Target](#), 66 F.Supp.3d at 1170.

317 The Plaintiffs also argue that [Hernandez Auto Painting](#) is not relevant here because it deals with the Georgia Insurance Commissioner’s enforcement authority, and does not address the question here. Pls.’ Br. in Opp’n to Defs.’ Mot. to Dismiss, at 64. However, the reasoning of that case is not limited to the specific statute at issue there. Instead, the court there addressed how to read silence as to the question of a private right of action in general. See [Hernandez Auto Painting](#), 312 Ga. App. at 761, 719 S.E.2d 597.

318 Defs.’ Mot. to Dismiss, at 66.

319 *Id.* at 66-67.

320 See, e.g., [Cal. Civ. Code § 1798.82\(a\)](#); [C.G.S.A. § 36a-701b\(b\)\(1\)](#).

321 [MD. CODE ANN., Com. Law § 14-3402\(a\)](#).

322 Consolidated Consumer Class Action Compl. ¶ 824.

323 Defs.’ Mot. to Dismiss, at 68.

324 Defs.’ Mot. to Dismiss, at 68.

325 *Id.*

326 [Target](#), 66 F.Supp.3d at 1166.

327 Pls.’ Br. in Opp’n to Defs.’ Mot. to Dismiss, at 66.

328 Defs.’ Mot. to Dismiss, at 69.

329 [In re Target Corp. Data Sec. Breach Litig.](#), 66 F.Supp.3d 1154, 1160 (D. Minn. 2014).

330 *Id.*

331 See [Griffin v. Dugger](#), 823 F.2d 1476, 1483 (11th Cir. 1987).

332 [Target](#), 66 F.Supp.3d at 1160; see also [Langan v. Johnson & Johnson Consumer Cos.](#), 897 F.3d 88, 93-96 (2d Cir. 2018) (noting that variations between class members’ claims are “substantive questions, not jurisdictional ones” and concluding that differences between state laws are questions of predominance for class certification, and not standing under Article III).

333 [O.C.G.A. § 13-6-11](#).

334 Pls.’ Br. in Opp’n to Defs.’ Mot. to Dismiss, at 69.

335 Defs.’ Mot. to Dismiss, at 69-70.

336 [Lewis v. D. Hays Trucking, Inc.](#), 701 F.Supp.2d 1300, 1313 (N.D. Ga. 2010) (“Plaintiff does not appear to seek any attorney’s fees based on resistance of the claim after the cause of action had arisen. Therefore, the basis for Plaintiff’s claim must be under the ‘bad faith’ prong of [§ 13–6–11](#).”).

337 *Id.*

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1.	Title
Section 2.	Purpose and Intent
Section 3.	Definitions
Section 4.	Information Security Program
Section 5.	Investigation of a Cybersecurity Event
Section 6.	Notification of a Cybersecurity Event
Section 7.	Power of Commissioner
Section 8.	Confidentiality
Section 9.	Exceptions
Section 10.	Penalties
Section 11.	Rules and Regulations [OPTIONAL]
Section 12.	Severability
Section 13.	Effective Date

Section 1. Title

This Act shall be known and may be cited as the “Insurance Data Security Law.”

Section 2. Purpose and Intent

- A. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.
- B. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Drafting Note: The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, *Cybersecurity Requirements for Financial Services Companies*, effective March 1, 2017, such Licensee is also in compliance with this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

- A. “Authorized Individual” means an individual known to and screened by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its Information Systems.
- B. “Commissioner” means the chief insurance regulatory official of the state.
- C. “Consumer” means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this State and whose Nonpublic Information is in a Licensee’s possession, custody, or control.
- D. “Cybersecurity Event” means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System.

The term “Cybersecurity Event” does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

- E. “Department” means the [insert name of insurance regulatory body].
- F. “Encrypted” means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.
- G. “Information Security Program” means the administrative, technical, and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information.
- H. “Information System” means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.
- I. “Licensee” means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.
- J. “Multi-Factor Authentication” means authentication through verification of at least two of the following types of authentication factors:
 - (1) Knowledge factors, such as a password; or
 - (2) Possession factors, such as a token or text message on a mobile phone; or
 - (3) Inherence factors, such as a biometric characteristic.
- K. “Nonpublic Information” means information that is not Publicly Available Information and is:
 - (1) Business related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Licensee;
 - (2) Any information concerning a Consumer which because of name, number, personal mark, or other identifier can be used to identify such Consumer, in combination with any one or more of the following data elements:
 - (a) Social Security number,
 - (b) Driver’s license number or non-driver identification card number,
 - (c) Account number, credit or debit card number,
 - (d) Any security code, access code or password that would permit access to a Consumer’s financial account, or
 - (e) Biometric records;
 - (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a Consumer and that relates to
 - (a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer's family,
 - (b) The provision of health care to any Consumer, or
 - (c) Payment for the provision of health care to any Consumer.

- L. “Person” means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.
- M. “Publicly Available Information” means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

For the purposes of this definition, a Licensee has a reasonable basis to believe that information is lawfully made available to the general public if the Licensee has taken steps to determine:
 - (1) That the information is of the type that is available to the general public; and
 - (2) Whether a Consumer can direct that the information not be made available to the general public and, if so, that such Consumer has not done so.
- N. “Risk Assessment” means the Risk Assessment that each Licensee is required to conduct under Section 4C of this Act.
- O. “State” means [adopting state].
- P. “Third-Party Service Provider” means a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee.

Section 4. Information Security Program

- A. Implementation of an Information Security Program

Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee’s activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee’s possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive written Information Security Program based on the Licensee’s Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee’s Information System.
- B. Objectives of Information Security Program

A Licensee’s Information Security Program shall be designed to:
 - (1) Protect the security and confidentiality of Nonpublic Information and the security of the Information System;
 - (2) Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System;
 - (3) Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and
 - (4) Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.
- C. Risk Assessment

The Licensee shall:
 - (1) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the Information Security Program;

- (2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers;
- (3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;
- (4) Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:
 - (a) Employee training and management;
 - (b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and
 - (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and
- (5) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Risk Management

Based on its Risk Assessment, the Licensee shall:

- (1) Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control.
- (2) Determine which security measures listed below are appropriate and implement such security measures.
 - (a) Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;
 - (b) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;
 - (c) Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;
 - (d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;
 - (e) Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;
 - (f) Modify the Information System in accordance with the Licensee's Information Security Program;

- (g) Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;
 - (h) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;
 - (i) Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;
 - (j) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and
 - (k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.
- (3) Include cybersecurity risks in the Licensee’s enterprise risk management process.
 - (4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and
 - (5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.

E. Oversight by Board of Directors

If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

- (1) Require the Licensee’s executive management or its delegates to develop, implement, and maintain the Licensee’s Information Security Program;
- (2) Require the Licensee’s executive management or its delegates to report in writing at least annually, the following information:
 - (a) The overall status of the Information Security Program and the Licensee’s compliance with this Act; and
 - (b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management’s responses thereto, and recommendations for changes in the Information Security Program.
- (3) If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee’s Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.

F. Oversight of Third-Party Service Provider Arrangements

- (1) A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and
- (2) A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.

G. Program Adjustments

The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.

H. Incident Response Plan

- (1) As part of its Information Security Program, each Licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity, or availability of Nonpublic Information in its possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations.
- (2) Such incident response plan shall address the following areas:
 - (a) The internal process for responding to a Cybersecurity Event;
 - (b) The goals of the incident response plan;
 - (c) The definition of clear roles, responsibilities and levels of decision-making authority;
 - (d) External and internal communications and information sharing;
 - (e) Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
 - (f) Documentation and reporting regarding Cybersecurity Events and related incident response activities; and
 - (g) The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

I. Annual Certification to Commissioner of Domiciliary State

Annually, each insurer domiciled in this State shall submit to the Commissioner, a written statement by February 15, certifying that the insurer is in compliance with the requirements set forth in Section 4 of this Act. Each insurer shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commissioner.

Section 5. Investigation of a Cybersecurity Event

- A. If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.
- B. During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:
 - (1) Determine whether a Cybersecurity Event has occurred;
 - (2) Assess the nature and scope of the Cybersecurity Event;
 - (3) Identify any Nonpublic Information that may have been involved in the Cybersecurity Event; and

- (4) Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.
- C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will complete the steps listed in Section 5B above or confirm and document that the Third-Party Service Provider has completed those steps.
- D. The Licensee shall maintain records concerning all Cybersecurity Events for a period of at least five years from the date of the Cybersecurity Event and shall produce those records upon demand of the Commissioner.

Section 6. Notification of a Cybersecurity Event

A. Notification to the Commissioner

Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met:

- (1) This State is the Licensee's state of domicile, in the case of an insurer, or this State is the Licensee's home state, in the case of a producer, as those terms are defined in [insert reference to Producer Licensing Model Act]; or
 - (2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this State and that is either of the following:
 - (a) A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or
 - (b) A Cybersecurity Event that has a reasonable likelihood of materially harming:
 - (i) Any Consumer residing in this State; or
 - (ii) Any material part of the normal operation(s) of the Licensee.
- B. The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.
- (1) Date of the Cybersecurity Event;
 - (2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any;
 - (3) How the Cybersecurity Event was discovered;
 - (4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;
 - (5) The identity of the source of the Cybersecurity Event;
 - (6) Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

- (7) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;
 - (8) The period during which the Information System was compromised by the Cybersecurity Event;
 - (9) The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;
 - (10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
 - (11) Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur;
 - (12) A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event; and
 - (13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.
- C. Notification to Consumers. Licensee shall comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when a Licensee is required to notify the Commissioner under Section 6A.
- D. Notice Regarding Cybersecurity Events of Third-Party Service Providers
- (1) In the case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, of which the Licensee has become aware, the Licensee shall treat such event as it would under Section 6A.
 - (2) The computation of Licensee's deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.
 - (3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third-Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.
- E. Notice Regarding Cybersecurity Events of Reinsurers to Insurers
- (1) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred.
 - (b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.
 - (2) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred.

- (b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state's breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

F. Notice Regarding Cybersecurity Events of Insurers to Producers of Record

In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected Consumers as soon as practicable as directed by the Commissioner.

The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.

Section 7. Power of Commissioner

- A. The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].
- B. Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this State which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.

Section 8. Confidentiality

- A. Any documents, materials or other information in the control or possession of the Department that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section 4I, Section 6B(2), (3), (4), (5), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.
- B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A.
- C. In order to assist in the performance of the Commissioner's duties under this Act, the Commissioner:
 - (1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;
 - (2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;

- (3) May share documents, materials or other information subject to Section 8A, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; and
 - (4) May enter into agreements governing sharing and use of information consistent with this subsection.
- D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in Section 8C.
- E. Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 9. Exceptions

- A. The following exceptions shall apply to this Act:
- (1) A Licensee with fewer than ten employees, including any independent contractors, is exempt from Section 4 of this Act;
 - (2) A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee is compliant with, and submits a written statement certifying its compliance with, the same;
 - (3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 and need not develop its own Information Security Program to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.
- B. In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.

Section 10. Penalties

In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].

Section 11. Rules and Regulations [OPTIONAL]

The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act.

Drafting Note: This provision is applicable only to states requiring this language.

Section 12. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 13. Effective Date

This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC).

2017 4th Quarter (adopted by Executive/Plenary via conference call)

This page is intentionally left blank

INSURANCE DATA SECURITY MODEL LAW

This chart is intended to provide readers with additional information to more easily access state statutes, regulations, bulletins or administrative rulings related to the NAIC model. Such guidance provides readers with a starting point from which they may review how each state has addressed the model and the topic being covered. The NAIC Legal Division has reviewed each state’s activity in this area and has determined whether the citation most appropriately fits in the Model Adoption column or Related State Activity column based on the definitions listed below. The NAIC’s interpretation may or may not be shared by the individual states or by interested readers.

This chart does not constitute a formal legal opinion by the NAIC staff on the provisions of state law and should not be relied upon as such. Nor does this state page reflect a determination as to whether a state meets any applicable accreditation standards. Every effort has been made to provide correct and accurate summaries to assist readers in locating useful information. Readers should consult state law for further details and for the most current information.

INSURANCE DATA SECURITY MODEL LAW

This page is intentionally left blank

INSURANCE DATA SECURITY MODEL LAW

KEY:

MODEL ADOPTION: States that have citations identified in this column adopted the most recent version of the NAIC model in a **substantially similar manner**. This requires states to adopt the model in its entirety but does allow for variations in style and format. States that have adopted portions of the current NAIC model will be included in this column with an explanatory note.

RELATED STATE ACTIVITY: Examples of Related State Activity include but are not limited to: older versions of the NAIC model, statutes or regulations addressing the same subject matter, or other administrative guidance such as bulletins and notices. States that have citations identified in this column **only** (and nothing listed in the Model Adoption column) have **not** adopted the most recent version of the NAIC model in a **substantially similar manner**.

NO CURRENT ACTIVITY: No state activity on the topic as of the date of the most recent update. This includes states that have repealed legislation as well as states that have never adopted legislation.

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
Alabama	ALA. CODE § 27-62-1 to 27-62-12 (2019).	
Alaska	NO CURRENT ACTIVITY	
American Samoa	NO CURRENT ACTIVITY	
Arizona	NO CURRENT ACTIVITY	
Arkansas	NO CURRENT ACTIVITY	
California	NO CURRENT ACTIVITY	
Colorado	NO CURRENT ACTIVITY	
Connecticut	CONN. GEN. STAT. ANN. § P.A. 19-117, § 230 (2019).	
Delaware	DEL. CODE ANN. tit. 18, §§ 8601 to 8611 (2019).	
District of Columbia	NO CURRENT ACTIVITY	
Florida	NO CURRENT ACTIVITY	
Georgia	NO CURRENT ACTIVITY	
Guam	NO CURRENT ACTIVITY	

INSURANCE DATA SECURITY MODEL LAW

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
Hawaii	NO CURRENT ACTIVITY	
Idaho	NO CURRENT ACTIVITY	
Illinois	NO CURRENT ACTIVITY	
Indiana	NO CURRENT ACTIVITY	
Iowa	NO CURRENT ACTIVITY	
Kansas	NO CURRENT ACTIVITY	
Kentucky	NO CURRENT ACTIVITY	
Louisiana	NO CURRENT ACTIVITY	
Maine	NO CURRENT ACTIVITY	
Maryland		S.B. No. 30 (2019); BULLETIN 2019-14 (2019).
Massachusetts	NO CURRENT ACTIVITY	
Michigan	MICH. COMP. LAWS §§ 500.550 to 500.565 (2018).	
Minnesota	NO CURRENT ACTIVITY	
Mississippi	S.B. No. 2831 (2019).	
Missouri	NO CURRENT ACTIVITY	
Montana	NO CURRENT ACTIVITY	
Nebraska	NO CURRENT ACTIVITY	
Nevada	NO CURRENT ACTIVITY	
New Hampshire	N.H. REV. STAT. ANN. §§ 420-P:1 to 420-P:14; §§ 309:2 to 309:3 (2019).	
New Jersey	NO CURRENT ACTIVITY	
New Mexico	NO CURRENT ACTIVITY	

INSURANCE DATA SECURITY MODEL LAW

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
New York		N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).
North Carolina	NO CURRENT ACTIVITY	
North Dakota	NO CURRENT ACTIVITY	
Northern Marianas	NO CURRENT ACTIVITY	
Ohio	OHIO REV. CODE ANN. §§ 3965.01 to 3965.11 (2018).	
Oklahoma	NO CURRENT ACTIVITY	
Oregon	NO CURRENT ACTIVITY	
Pennsylvania	NO CURRENT ACTIVITY	
Puerto Rico	NO CURRENT ACTIVITY	
Rhode Island	NO CURRENT ACTIVITY	
South Carolina	S.C. CODE ANN. §§ 38-99-10 to 38-99-100 (2018).	
South Dakota	NO CURRENT ACTIVITY	
Tennessee	NO CURRENT ACTIVITY	
Texas	NO CURRENT ACTIVITY	
Utah	NO CURRENT ACTIVITY	
Vermont	NO CURRENT ACTIVITY	
Virgin Islands	NO CURRENT ACTIVITY	
Virginia	NO CURRENT ACTIVITY	
Washington	NO CURRENT ACTIVITY	
West Virginia	NO CURRENT ACTIVITY	

INSURANCE DATA SECURITY MODEL LAW

NAIC MEMBER	MODEL ADOPTION	RELATED STATE ACTIVITY
Wisconsin	NO CURRENT ACTIVITY	
Wyoming	NO CURRENT ACTIVITY	

SENATE BILL NO. 361

BY SENATOR WALSWORTH

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

AN ACT

To amend and reenact R.S. 51:3073(2) and (4)(a) and 3074, relative to the Database Security Breach Notification Law; to provide for the protection of personal information; to require certain security procedures and practices; to provide for notification requirements; to provide relative to violations; to provide for definitions; and to provide for related matters.

Be it enacted by the Legislature of Louisiana:

Section 1. R.S. 51:3073(2) and (4)(a) and 3074 are hereby amended and reenacted to read as follows:

§3073. Definitions

As used in this Chapter, the following terms shall have the following meanings:

* * *

(2) "Breach of the security of the system" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable ~~basis to conclude has resulted~~ **likelihood to result** in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized disclosure.

* * *

(4)(a) "Personal information" means ~~an individual's~~ **the** first name or first initial and last name **of an individual resident of this state** in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

- 1 (i) Social security number.
- 2 (ii) Driver's license number or state identification card number.
- 3 (iii) Account number, credit or debit card number, in combination with any
- 4 required security code, access code, or password that would permit access to an
- 5 individual's financial account.

6 (iv) Passport number.

7 (v) Biometric data. "Biometric data" means data generated by automatic
 8 measurements of an individual's biological characteristics, such as fingerprints,
 9 voice print, eye retina or iris, or other unique biological characteristic that is
 10 used by the owner or licensee to uniquely authenticate an individual's identity
 11 when the individual accesses a system or account.

12 * * *

13 §3074. ~~Disclosure~~ **Protection of personal information; disclosure** upon breach in
 14 the security of personal information; notification requirements;
 15 exemption

16 A. Any person that conducts business in the state or that owns or licenses
 17 computerized data that includes personal information, or any agency that owns
 18 or licenses computerized data that includes personal information, shall
 19 implement and maintain reasonable security procedures and practices
 20 appropriate to the nature of the information to protect the personal information
 21 from unauthorized access, destruction, use, modification, or disclosure.

22 B. Any person that conducts business in the state or that owns or licenses
 23 computerized data that includes personal information, or any agency that owns
 24 or licenses computerized data that includes personal information shall take all
 25 reasonable steps to destroy or arrange for the destruction of the records within
 26 its custody or control containing personal information that is no longer to be
 27 retained by the person or business by shredding, erasing, or otherwise
 28 modifying the personal information in the records to make it unreadable or
 29 undecipherable through any means.

30 C. Any person that conducts business in the state or that owns or licenses

1 computerized data that includes personal information, or any agency that owns or
2 licenses computerized data that includes personal information, shall, following
3 discovery of a breach in the security of the system containing such data, notify any
4 resident of the state whose personal information was, or is reasonably believed to
5 have been, acquired by an unauthorized person.

6 ~~B.D.~~ Any agency or person that maintains computerized data that includes
7 personal information that the agency or person does not own shall notify the owner
8 or licensee of the information if the personal information was, or is reasonably
9 believed to have been, acquired by an unauthorized person through a breach of
10 security of the system containing such data, following discovery by the agency or
11 person of a breach of security of the system.

12 ~~E.~~ The notification required pursuant to Subsections ~~A and B~~ **C and D** of
13 this Section shall be made in the most expedient time possible and without
14 unreasonable delay **but not later than sixty days from the discovery of the**
15 **breach**, consistent with the legitimate needs of law enforcement, as provided in
16 Subsection ~~D~~ **F** of this Section, or any measures necessary to determine the scope of
17 the breach, prevent further disclosures, and restore the reasonable integrity of the
18 data system. **When notification required pursuant to Subsections C and D of this**
19 **Section is delayed pursuant to Subsection F of this Section or due to a**
20 **determination by the person or agency that measures are necessary to**
21 **determine the scope of the breach, prevent further disclosures, and restore the**
22 **reasonable integrity of the data system, the person or agency shall provide the**
23 **attorney general the reasons for the delay in writing within the sixty day**
24 **notification period provided in this Subsection. Upon receipt of the written**
25 **reasons, the attorney general shall allow a reasonable extension of time to**
26 **provide the notification required in Subsections C and D of this Section.**

27 ~~D.F.~~ If a law enforcement agency determines that the notification required
28 under this Section would impede a criminal investigation, such notification may be
29 delayed until such law enforcement agency determines that the notification will no
30 longer compromise such investigation.

1 ~~E.G.~~ Notification may be provided by one of the following methods:

2 (1) Written notification.

3 (2) Electronic notification, if the notification provided is consistent with the
4 provisions regarding electronic records and signatures set forth in 15 ~~USE~~ U.S.C.
5 7001.

6 (3) Substitute notification, if an agency or person demonstrates that the cost
7 of providing notification would exceed ~~two hundred fifty~~ **one hundred** thousand
8 dollars, or that the affected class of persons to be notified exceeds ~~five~~ **one** hundred
9 thousand, or the agency or person does not have sufficient contact information.
10 Substitute notification shall consist of all of the following:

11 (a) E-mail notification when the agency or person has an e-mail address for
12 the subject persons.

13 (b) Conspicuous posting of the notification on the Internet site of the agency
14 or person, if an Internet site is maintained.

15 (c) Notification to major statewide media.

16 ~~F.H.~~ Notwithstanding Subsection ~~E G~~ of this Section, an agency or person
17 that maintains a notification procedure as part of its information security policy for
18 the treatment of personal information which is otherwise consistent with the timing
19 requirements of this Section shall be ~~deemed~~ **considered** to be in compliance with
20 the notification requirements of this Section if the agency or person notifies subject
21 persons in accordance with the policy and procedure in the event of a breach of
22 security of the system.

23 ~~G. Notification under this title is not required if after a reasonable~~
24 ~~investigation the person or business determines that there is no reasonable likelihood~~
25 ~~of harm to customers.~~

26 **I. Notification as provided in this Section shall not be required if after a**
27 **reasonable investigation, the person or business determines that there is no**
28 **reasonable likelihood of harm to the residents of this state. The person or**
29 **business shall retain a copy of the written determination and supporting**
30 **documentation for five years from the date of discovery of the breach of the**

1 security system. If requested in writing, the person or business shall send a copy
 2 of the written determination and supporting documentation to the attorney
 3 general no later than thirty days from the date of receipt of the request. The
 4 provisions of R.S. 51:1404(A)(1)(c) shall apply to a written determination and
 5 supporting documentation sent to the attorney general pursuant to this
 6 Subsection.

7 J. A violation of a provision of this Chapter shall constitute an unfair act
 8 or practice pursuant to R.S. 51:1405(A).

 PRESIDENT OF THE SENATE

 SPEAKER OF THE HOUSE OF REPRESENTATIVES

 GOVERNOR OF THE STATE OF LOUISIANA

APPROVED: _____