Virginia's New Consumer Data Protection Act, Va Code § 59.1-571

George Mason American Inn of Court
January 18, 2022

Judge Judith Wheat – Arlington Co. Cir. Court
Nick Gehrig – Redmon, Peyton & Braswell, LLP
Malcolm Thomas – Bean, Kinney & Korman, PC
Cristina Del Rosso – GMU Law
Jacob Hopkins – GMU Law
Douglas Horn – GMU Law
Raymond Yang – GMU Law
Tom Urban – Fletcher, Heald & Hildreth, PLC

Materials for Presentation –
Virginia's New Consumer Data Protection Act

1. **Consumer Data Protection Act, Va. Code § 59.1-571, et seq.**

2. **Final Report of the Virginia Consumer Data Protection Act Working group of the Joint Commission on Technology and Science**

3. **Summary of the Consumer Data Protection Act – Morrison & Foerster (September 2021)**

4. **Comparison of Virginia Consumer Data Protection Act, California Consumer Privacy Act, and the European Union's General Data Protection Regulation**

5. **GMU Scalia Law School Law & Economics Report on Private Litigation Under the California Consumer Privacy Act (May 2021)**

6. ***Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020).**

7. ***Gardiner v. Walmart Inc.*, No. 20-CV-04618-JSW, 2021 WL 2520103, at *2 (N.D. Cal. Mar. 5, 2021).**

8. ***In re Blackbaud, Inc., Customer Data Breach Litig.,* No. 3:20-MN-02972-JMC, 2021 WL 3568394, at *5 (D.S.C. Aug. 12, 2021).**

EXHIBIT 1

CHAPTER 52.
CONSUMER DATA PROTECTION ACT.

§59.1-571. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-573, is the same consumer exercising such consumer rights with respect to the personal data at issue.

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

"Business associate" means the same meaning as the term established by HIPAA.

"Child" means any natural person younger than 13 years of age.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Covered entity" means the same as the term is established by HIPAA.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. A controller that possesses "de-identified data" shall comply with the requirements of subsection A of §59.1-577.

"Fund" means the Consumer Privacy Fund established pursuant to §59.1-581.

"Health record" means the same as that term is defined in §32.1-127.1:03.

"Health care provider" means the same as that term is defined in §32.1-276.3.

"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §1320d et seq.).

"Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

"Institution of higher education" means a public institution and private institution of higher education, as those terms are defined in §23.1-100.

"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation Act (§13.1-801 et seq.) or any organization exempt from taxation under §501(c)(3), 501(c)(6), or 501 (c)(12) of the Internal Revenue Code, and any subsidiaries and affiliates of entities organized pursuant to Chapter 9.1 (§56-231.15 et seq.) of Title 56.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

"Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

"Processor" means a natural or legal entity that processes personal data on behalf of a controller.

"Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Protected health information" means the same as the term is established by HIPAA.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include:

1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;

2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

3. The disclosure or transfer of personal data to an affiliate of the controller;

4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or

5. The disclosure or transfer of personal data to a third party 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 controller's assets.

"Sensitive data" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

3. The personal data collected from a known child; or

4. Precise geolocation data.

"State agency" means the same as that term is defined in §2.2-307.

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include:

1. Advertisements based on activities within a controller's own websites or online applications;

2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

"Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

§59.1-572. Scope; exemptions.

A. This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

B. This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. §6801 et seq.); (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization; or (v) institution of higher education.

C. The following information and data is exempt from this chapter:

1. Protected health information under HIPAA;

2. Health records for purposes of Title 32.1;

3. Patient identifying information for purposes of 42 U.S.C. §290dd-2;

4. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law;

5. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. §11101 et seq.);

6. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. §299b-21 et seq.);

7. Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

8. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. §290dd-2;

9. Information used only for public health activities and purposes as authorized by HIPAA;

10. The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. §1681 et seq.);

11. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. §2721 et seq.);

12. Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. §1232g et seq.);

13. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. §2001 et seq.); and

14. Data processed or maintained (i) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role; (ii) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual under clause (i) and used for the purposes of administering those benefits.

D. Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. §6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

§59.1-573. Personal data rights; consumers.

A. A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;

2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

3. To delete personal data provided by or obtained about the consumer;

4. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

B. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to subsection A as follows:

1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in §59.1-573 A. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

2. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection C.

3. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

4. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action

under subsection A and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

C. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision B 2. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

§59.1-574. Data controller responsibilities; transparency.

A. A controller shall:

1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

3. Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;

4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to §59.1-573 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

5. Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. §6501 et seq.).

B. Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights pursuant to § 59.1-573 shall be deemed contrary to public policy and shall be void and unenforceable.

C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

1. The categories of personal data processed by the controller;

2. The purpose for processing personal data;

3. How consumers may exercise their consumer rights pursuant §59.1-573, including how a consumer may appeal a controller's decision with regard to the consumer's request;

4. The categories of personal data that the controller shares with third parties, if any; and

5. The categories of third parties, if any, with whom the controller shares personal data.

D. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

E. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to §59.1-573 but may require a consumer to use an existing account.

§59.1-575. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to §59.1-573.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to §18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to §59.1-576.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

§59.1-576. Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;

2. The sale of personal data;

3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

4. The processing of sensitive data; and

5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

C. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in §59.1-574. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

D. A single data protection assessment may address a comparable set of processing operations that include similar activities.

E. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

F. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

§59.1-577. Processing de-identified data; exemptions.

A. The controller in possession of de-identified data shall:

1. Take reasonable measures to ensure that the data cannot be associated with a natural person;

2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

B. Nothing in this chapter shall be construed to (i) require a controller or processor to re-identify de-identified data or pseudonymous data or (ii) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

C. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to §59.1-573, if all of the following are true:

1. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

2. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

D. The consumer rights contained in subdivisions A 1 through 4 of §59.1-573 and §59.1-574 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

§59.1-578. Limitations.

A. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

1. Comply with federal, state, or local laws, rules, or regulations;

2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

3. Cooperate with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

4. Investigate, establish, exercise, prepare for, or defend legal claims;

5. Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

6. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

8. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine: (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

9. Assist another controller, processor, or third party with any of the obligations under this subsection.

B. The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to:

1. Conduct internal research to develop, improve, or repair products, services, or technology;

2. Effectuate a product recall;

3. Identify and repair technical errors that impair existing or intended functionality; or

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

C. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the Commonwealth. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the Commonwealth as part of a privileged communication.

D. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives such personal data.

E. Nothing in this chapter shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

F. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

1. Reasonably necessary and proportionate to the purposes listed in this section; and

2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection B shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

G. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection F.

H. Processing personal data for the purposes expressly identified in subdivisions A 1 through 9 shall not solely make an entity a controller with respect to such processing.

§59.1-579. Investigative authority.

Whenever the Attorney General has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the Attorney General is empowered to issue a civil investigative demand. The provisions of §59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued under this section.

§59.1-580. Enforcement; civil penalty; expenses.

A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

B. Prior to initiating any action under this chapter, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period, the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

C. If a controller or processor continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to $7,500 for each violation under this chapter.

D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

§59.1-581. Consumer Privacy Fund.

There is hereby created in the state treasury a special nonreverting fund to be known as the Consumer Privacy Fund. The Fund shall be established on the books of the Comptroller. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Fund. Interest earned on moneys in the Fund shall remain in the Fund and be credited to it. Any moneys remaining in the Fund, including interest thereon, at the end of each fiscal year shall not revert to the general fund but shall remain in the Fund. Moneys in the Fund shall be used to support the work of the Office of the Attorney General to enforce the provisions of this chapter, subject to appropriation.

2. The Chairman of the Joint Commission on Technology and Science shall create a work group composed of the Secretary of Commerce and Trade, the Secretary of Administration, the Attorney General, the Chairman of the Senate Committee on Transportation, representatives of businesses who control or process personal data of at least 100,000 persons, and consumer rights advocates. The work group shall review the provisions of this act and issues related to its implementation. The Chairman of the Joint Commission on Technology and Science shall submit the work group's findings, best practices, and recommendations regarding the implementation of this act to the Chairmen of the Senate Committee on General Laws and Technology and the House Committee on Communications, Technology and Innovation no later than November 1, 2021.

3. That any reference to federal law or statute in this act shall be deemed to include any accompanying rules or regulations or exemptions thereto. Further, this enactment is declaratory of existing law.

4. That the provisions of the first and third enactments of this act shall become effective on January 1, 2023.

EXHIBIT 2

Final Report

Joint Commission on Technology and Science

Virginia Consumer Data Protection Act Work Group

2021 Final Report

http://dls.virginia.gov/commission/jcots.htm

The Virginia Consumer Data Protection Act Work Group (the Work Group) of the Joint Commission on Technology and Science (the Commission) met six times with Delegate C.E. Cliff Hayes, Jr., chair, presiding. The Work Group was created pursuant to the second enactments of HB 2307 and SB 1392 (2021, Special Session I), known as the Virginia Consumer Data Protection Act (VCDPA), to study findings, best practices, and recommendations prior to the January 2023 implementation of the Act. Materials presented at the meeting are accessible through the *Commission's meetings webpage*. Full videos of each meeting are archived on the *House video streaming webpage*.

Information presented at the meetings is summarized here.

Membership

Delegate C.E. Cliff Hayes, Jr. (chair)

Senator David W. Marsden

Secretary of Commerce & Trade Brian Ball (represented by Evan Feinman)

Secretary of Administration Grindly Johnson (represented by Marcus Thornton)

Attorney General Mark Herring (represented by Samuel Towell)

Gill Bland, Urban League of Hampton Roads

Elizabeth Falcone, U.S. Senator Mark Warner (represented by Rafi Martinez & Kate Landers)

Stacey Gray, Future of Privacy Forum

Jim Halpert, State Privacy & Security Coalition

Keir Lamont, Computer & Communications Industry Association

Executive Summary

The following are points of emphasis that arose during the six Work Group meetings:

- Consider leadership, outside of the Office of Attorney General, to lead an educational initiative to assist small to medium-sized businesses in complying with the VCDPA;
- Submit a budget amendment to fund two staff members, and two attorneys through general funds to lead enforcement of the VCDPA from day one of enactment;
- Replace the Consumer Privacy Fund with the existing general funds;
- Allow the Office of the Attorney General to pursue actual damages based on consumer harm, should they exist;
- Employ an "ability to cure" option for violations, should a potential cure exist;
- Authorize consumers to assert and requiring companies to honor a global opt-out setting as a single-step for consumers to opt-out of data collection;
- Sunset the "right to cure" provision after the initial years of VCDPA enactment to prevent companies from exploiting this provision;
- Amend the "right to delete" provision to be a "right to opt out of sale" provision in order to promote compliance and restrict further dissemination of consumer personal data;
- Consider a narrow exemption for § 501(c)(4) nonprofit organizations established to detect or prevent insurance-related crime or fraud;
- Study specific data privacy protection provisions for children;
- Request an annual report from the Office of the Attorney General on enforcement of the VCDPA;
- Encourage the development of third-party software and browser extensions to allow users to universally opt out of data collection, rather than individually from each website;
- Recruit nonprofit consumer and privacy organizations to address concerns with the definitions of "sale," "personal data," and "publicly available information" in the VCDPA;
- Consider whether the definition of "sensitive data" should include general demographic data used to promote diversity and outreach to underserved populations;
- Create a website dedicated to educating consumers about their rights under the VCDPA;
- Direct an agency to promulgate regulations because the current VCDPA does not allow the Office of the Attorney General to promulgate regulations; and
- Post and promote sample data protection forms on an educational website to provide guidance to smaller businesses seeking to comply with the VCDPA.

Delegate Hayes and Senator Marsden will present the Work Group's recommendations based on these points of emphasis during the upcoming legislative session.

The Work Group met virtually on June 14, 2021, to discuss the following topics:

Presentation: Timeline of Virginia Consumer Data Protection Act

Delegate C.E. Cliff Hayes, Jr.

Delegate Hayes described the process of writing the Virginia Consumer Data Protection Act (VCDPA) beginning in January 2020 and the General Assembly passing the legislation (HB 2307 [Hayes] and SB 1392 [Marsden]) during the 2021 Special Session I. He explained that Virginia is only the second state to pass comprehensive general data privacy legislation, following the passage of the California Consumer Privacy Act in 2018. The VCDPA was modeled on SB 5062 in Washington, which failed to pass the Washington State Legislature earlier this year. As part of the enactment of the VCDPA, the General Assembly directed the Joint Commission to create the Work Group to review the provisions of the act and issues related to its implementation.

Presentation: Provisions of the VCDPA

Hassan Abdelhalim, Attorney, Division of Legislative Services
David Barry, Attorney, Division of Legislative Services

Mr. Abdelhalim and Mr. Barry described the provisions of the VCDPA, including the data, controllers, and processors that are covered by the VCDPA and data that is exempted by federal law; rights of customers to control their data; limitations on requirements of controllers and processors; and enforcement authority. They also outlined the responsibilities of the Work Group and the effective date of the VCDPA as well as proposed future dates for Work Group meetings.

Public Comment

Work Group member Jim Halpert said that because the Attorney General's office is tasked with enforcement of the VCDPA, the Work Group should consider what type of educational outreach should be done, particularly to small-sized and medium-sized businesses, to assist with compliance with the VCDPA.

Joint Commission member Delegate Kathy J. Byron asked for more information about the Washington privacy act. Delegate Hayes responded that the VCDPA was based on the Washington privacy act, but that the VCDPA omitted any reference to or regulation of facial recognition technology because that was a contributing factor to the Washington bill's failure to pass. He added that U.S. Representative Suzan DelBene from Washington has introduced legislation for federal regulation of data privacy.

The following is a summary of the information presented at the Work Group's meeting on July 12, 2021, in Richmond:

Presentation: Attorney General Presentation

Samuel Towell, Deputy Attorney General, Office of Attorney General

Mr. Towell presented on the Virginia Consumer Data Protection Act (the VCDPA) from the perspective of the Office of the Attorney General (OAG). Enforcement issues identified by the Attorney General include the ability to cure; funding; damages, penalties, expenses, and fees; and separating the educational campaign from the enforcement within the Office of the Attorney General. Mr. Towell noted that the VCDPA cannot fix issues such as the leaking of data after a breach and the sale of such data to a third party. A company seeking to address such a violation

will need to remedy the architecture that allowed the breach to occur within 30 days, he said. He also noted that funds to enforce the VCDPA are currently anemic. Members of the Work Group responded by recommending submitting a budget amendment during the next session of the General Assembly. Mr. Towell concluded by outlining the following recommendations on behalf of the OAG:

- Fund two attorney and two staff positions through general funds;
- Replace the Consumer Privacy Fund with existing general funds;
- Allow the OAG to pursue actual damages to consumers, to the extent they exist;
- Employ "ability to cure" for those violations in which a cure is possible; and
- Involve OAG as a piece, but not the lead, of an education campaign.

Public Comment

Dr. Maureen Mahoney, a senior analyst at Consumer Reports, Inc., requested that the Work Group consider requiring companies to honor browser privacy signals as a global opt out as a single step for consumers (similar to the California Consumer Privacy Act); a sunset on the right to cure to prevent companies from exploiting this provision; and continuing to close loopholes in the law as they arise, similar to California's ongoing efforts to strengthen the California Consumer Privacy Act.

The following is a summary of the information presented at the Work Group's meeting on August 17, 2021, in Richmond:

Topics Identified with Regard to Implementation of the VCDPA

Delegate Hayes led a discussion involving points of interest related to the Virginia Consumer Data Protection Act (the Act). Julien Nagarajan, representing LexisNexis, spoke on challenges of maintaining compliance identified with deleting original data that could be compiled through indirect collection at a later date. Mr. Nagarajan offered a solution of amending the "right to delete" provision as a "right to opt out of sale" provision in order to restrict the further dissemination of consumer personal data. The proposed language linking the "right to delete" to the "opt out" provision seeks to give consumers the peace of mind that if they request data deletion, their request will be honored. The Work Group requested specific language to consider be provided before the next meeting.

Tim Lynch and Richard DiZinno, representing the National Insurance Crime Bureau, asked the Work Group to consider a narrow exemption to the Act. Mr. Lynch sought to exempt § 501(c)(4) nonprofit organizations "established to detect or prevent insurance-related crime or fraud" from the Act. He clarified that the nonprofit that fits this definition is unique in its positioning as it's the only one of its kind that communicates between insurance agencies and law enforcement and compliance with the Act would significantly alter their obligations and alter operations. Some members of the Work Group requested specific language be submitted to the Work Group so that the members may better understand their request

Presentation: Governor's Administration Considerations

Evan Feinman, Chief Broadband Officer, Office of the Governor

Mr. Feinman, a member of the Work Group, presented on behalf of the Office of the Governor on issues related to implementing the Act. Mr. Feinman explained the following issues:

- The Act would be strengthened by addressing data privacy protections for children;
- A universal opt-out tool would improve the effectiveness of the Act for Virginia citizens;
- Addition of an annual report from the Office of Attorney General would create a lasting avenue to fine-tune enforcement and build public confidence in the law; and
- Some fine-tuning for the treatment of public records processors may be productive

Mr. Feinman asked the Work Group to encourage the development of third-party software options to allow users to universally opt out of data collection from all websites rather than expecting a consumer to individually opt out of each site they visit. Mr. Feinman highlighted that the availability of software to standardize this process would be more in line with consumer expectations of data privacy. Some members expressed concern with the feasibility of global opt-out provisions due to differences between opt-out provisions in data privacy laws across states.

At the conclusion of the presentations, members of the Work Group discussed next steps. Delegate Hayes reacted favorably to gathering presentations, language suggestions for alterations to the Act, and public comments and to make such information available to the Work Group and staff in preparation for the Work Group's final report.

Public Comment

During the public comment period, a representative from the Virginia Citizens Consumer Council outlined concerns with educating the public of their rights under the Act. A representative from the Consumer Federation of America sought to encourage further participation by nonprofit consumer and privacy organizations to address concerns with the definitions of sale, personal data, and publically available information.

The following is a summary of the information presented at the Work Group's meeting on September 13, 2021, in Richmond:

Topics Identified with Regard to Implementation of the VCDPA

Delegate Hayes led a discussion related to the Consumer Data Protection Act (the Act). Chris Oswald, representing the Association of National Advertisers, spoke on potential issues with the Act's definition of "sensitive data." He pointed out the difficulties of using demographic data to reach out to particular underserved populations if the provisions of the law define such data as sensitive. Members had questions about businesses that want to serve diverse and underserved populations and collect racial demographic information about them, which can be used by companies to track their targets, according to Mr. Oswald. He gave an example of allowing a marketer that wants to engage potential customers to ask consumers to opt in to this data collection. Some members pointed out that opt-in provisions for behavioral advertisers are an industry custom, although in the context of tracking diversity these provisions may not currently apply to the use of data for that purpose. Mr. Oswald concluded that he will follow up and incorporate these comments and suggestions into ongoing discussions with the Work Group

Members of the Work Group then discussed next steps. Delegate Hayes noted that member Dana Wiggins will be giving a presentation to the Work Group on the implementation of the Act. By November, the Work Group will draft and present a final report to the General Assembly. Members of the Work Group announced their choice of Delegate Hayes and Senator David W. Marsden to present legislation based on the findings of the Work Group during the upcoming session of the General Assembly.

The following is a summary of the information presented at the Work Group's meeting on October 13, 2021, in Richmond:

Topics Identified with Regard to Implementation of the VCDPA

Dana Wiggins, Virginia Poverty Law Center, Consumer Education

Ms. Wiggins stated that consumer education is paramount to consumer protection and suggested a dedicated website to educate consumers. She said polling and messaging and working with instructional designers will be helpful in educating consumers of the rights under the law. She recommended a browser extension as a global opt-out to exercise privacy rights. Ms. Wiggins concluded by reiterating the value of being clear about where the law does and doesn't meet consumer expectations to empower and educate consumers on the implementation of the law.

Members had questions about the browser extension, and Ms. Wiggins clarified that a tweak in the law will be needed to allow consumers an opportunity to opt out globally rather than individually opting out of each website. Some members had questions about the current state of the law and remedies of negligent consumer data violations. Samuel Towell, of the Office of the Attorney General, described the differences in available remedies under the Virginia Consumer Protection Act and the Virginia Consumer Data Protection Act (VCDPA). He noted that the VCDPA does not currently provide for a consumer to recover actual damages suffered from a violation of the VCDPA. Other legal theories may allow a consumer to recover through litigation unrelated to the VCDPA, but often the cost of such litigation in comparison to the potential recovery makes pursing such an option impractical. Additionally, Mr. Towell stated that the VCDPA does not allow for the Office of the Attorney General to promulgate regulations, and that in any litigated matter under the VCDPA, a judge would decide any monetary award.

At the conclusion of the presentation, members of the Work Group discussed next steps. Delegate Hayes noted that he will work with Senator David W. Marsden to suggest recommendations for funding the initial operations within the Office of the Attorney General. Specific recommendations will be made available prior to the final Work Group report due on November 1, 2021. Senator Marsden also encouraged future collaboration with other states while noting data protection legislation will not likely occur on the federal level.

Stacey Gray inquired about allowing written public comments. Staff confirmed that a notice will go out after the meeting and public comments will be made available to the members of the Work Group after the meeting.

The following is a summary of the information presented at the Work Group's meeting on

October 25, 2021, in Richmond:

Summary of Work Group

Delegate C.E. Cliff Hayes, Jr.

Delegate Hayes summarized the events leading to the creation of the Work Group. He noted that legislation in Washington state was a starting model for the effort to pass similar data privacy legislation in the Commonwealth and added that two important strategic distinctions that led to the successful passage of the Virginia Consumer Data Protection Act (VCDPA), as opposed to similar legislative efforts in other states other state efforts, remain the exclusion of facial recognition and the enforcement of the law by the Attorney General. He also emphasized the need for comprehensive consumer education about the VCDPA as well as fully funding attorneys and staff within the Office of the Attorney General (OAG) through the upcoming budget process. To that end, Delegate Hayes noted that there are plans to develop a website to educate consumers and offer contact information for the OAG. Senator David W. Marsden pointed out that the Commonwealth has developed the first workable data privacy bill on the state level. He stated that there will be a continuing effort to improve upon the bill during the upcoming legislative session.

Samuel Towell suggested minor changes to the structure of the Consumer Privacy Fund (the Fund) to facilitate funding from day one of the enactment of the VCDPA, noting that, as currently written, the Fund subsidizes enforcement of the VCDPA through the OAG.

Jim Halpert brought to the attention of the Work Group that there are currently minor differences in the requirements of data protection assessments required by the VCDPA as compared to European law. As part of a broader educational effort, he recommended providing sample forms as a guidance tool for smaller companies seeking to comply with the data protection assessments under the VCDPA. Stacey Gray endorsed this model as helpful, and Mr. Towell once again underscored the effectiveness of an office outside of the OAG as part of an initiative to educate consumers and businesses.

Kate Landers, on behalf of U.S. Senator Mark Warner's office, promoted the inclusion of a global privacy control to allow consumers to opt-out on a wide scale and assert their rights under the VCDPA.

Dana Wiggins requested formatting the final report to include a list of the recommendations discussed throughout the five Work Group meetings. Delegate Hayes responded that the report is in draft form and that the list of recommendations will be incorporated into the final version.

Closing Remarks

At the conclusion of the meeting, Delegate Hayes thanked staff and each member of the Work Group individually for their service. He said that the findings and final report will be distributed to members and staff upon completion. Delegate Hayes and Senator Marsden said that they will introduce the official recommendations of the Work Group during the upcoming session of the General Assembly.

For more information, see the *Joint Commission's website* or contact the Division of Legislative Services staff:

Hassan Abdelhalim, Attorney, DLS
habdelhalim @dls.virginia.gov
804-698-1868

EXHIBIT 3

THE VIRGINIA CONSUMER DATA PROTECTION ACT (VCDPA)

MORRISON FOERSTER

SEPTEMBER 2021

The VCDPA ("the Act") grants Virginia consumers individual rights and imposes corresponding obligations on covered businesses:

GDPR-LIKE CONTROLLER / PROCESSOR DISTINCTION

Like the EU GDPR, the Act distinguishes between:

Controllers: Entities that determine the purpose and means of processing personal data; and

Processors: Entities that process personal data on behalf of a controller. The Act imposes specific obligations and limitations on processors, and sets forth required contents of a written controller-processor contract.

INDIVIDUAL RIGHTS

1. **Right to Know / Access.** Consumers may request that a controller confirm whether it processes personal data relating to the individual and provide access to that personal data.
2. **Right to Correction.** Consumers may request that a controller correct inaccuracies in the consumer's personal data.
3. **Right to Deletion.** Consumers may request that a controller delete personal data *provided by or obtained about* the consumer.
   - *Note*: This is not limited to personal data collected *from* the consumer, and the Act does not contain specific deletion exceptions.
4. **Right to Data Portability.** Consumers may request to obtain a copy of the personal data *that they previously provided to a controller* in a portable and, to the extent technically feasible, readily usable format, where the processing is carried out by automated means.
5. **Right to Opt Out.** Consumers may request to opt out of a controller's processing of their personal data for targeted advertising, sale, or automated profiling in furtherance of decisions that produce significant effects.
6. **Right to Appeal.** Consumers may appeal a controller's denial of their individual rights requests. See "Controllers' Obligations" for more.

CONTROLLERS' OBLIGATIONS

Data Minimization. Controllers must limit their collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes for which the data are processed, as disclosed to the consumer.

Purpose Limitation. Controllers are generally prohibited from processing personal data for purposes that are not reasonably necessary to, or compatible with, the disclosed purposes without the consumer's consent.

Notice. Controllers must provide consumers with meaningful notice regarding the personal data they process, the personal data they share with third parties, if applicable, and how consumers may exercise their rights under the Act, including the right to appeal.

Consent. Controllers must obtain consent to process a consumer's sensitive personal data (see flip side) and may only process the personal data of children *under the age of 13* in accordance with COPPA.

Data Security. Controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect personal data.

Non-Discrimination. Controllers may not process personal data in violation of state or federal discrimination laws, nor discriminate against consumers for exercising their rights under the Act.

Data Protection Assessments. Controllers must conduct and document data protection assessments for certain high-risk processing activities and make such assessments available to the Attorney General upon request.

Appeals Process. Controllers must establish a process for consumers to appeal denials of individual rights requests and make the process conspicuously available to consumers. A controller that denies an appeal must provide the individual with a mechanism to contact the Virginia AG.

THE VIRGINIA CONSUMER DATA PROTECTION ACT (VCDPA)

MORRISON FOERSTER

WHO MUST COMPLY?

The Act applies to entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents *and* that:

- Control or process personal data of at least **100,000 consumers who are VA residents** in a calendar year; *or*
- Control or process the personal data of at least **25,000 consumers who are VA residents** *and* derive over **50% of gross revenue** from the sale of personal data.

KEY DEFINITIONS

Consumer: a Virginia resident, but only to the extent that the individual is acting in an individual or household context.

- ➢ Excludes individuals acting in a B2B or employment context.

Personal Data: information linked or reasonably linkable to an identified or identifiable *individual* (not a household or device).

- ➢ Excludes de-identified and publicly available data, but note that a controller in possession of de-identified data must publicly commit that it will not attempt re-identification, among other conditions.

Sensitive Data: (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical diagnoses, sexual orientation, or citizenship or immigration status; (ii) genetic or biometric data for identification purposes; (iii) personal data collected from a child under 13 years of age; and (iv) precise geolocation data.

Sale: the exchange of personal data from a controller to a third party *for monetary consideration.*

- ➢ Excludes sharing data with affiliates and certain other sharing.

EXCEPTIONS

Entities: The Act exempts non-profit organizations, institutions of higher education, utilities, financial institutions subject to Title V of the GLBA, and HIPAA-covered entities and business associates.

Types of Personal Data: The Act exempts personal data created or maintained in the employment context or for purposes of select federal laws, including HIPAA, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and the Driver's Privacy Protection Act.

Permitted Processing: The Act does not restrict a controller or processor's ability to comply with laws or regulations or provide a product or service specifically requested by a consumer, among other purposes.

ENFORCEMENT

- ✓ **Virginia AG** has enforcement authority.
- ✓ **No private right of action**, even following data security incidents.
- ✓ Businesses have a **30-day period** to cure alleged violations, upon receipt of AG notice.
- ✓ Thereafter, AG may seek civil penalties of up to **$7,500 per** violation, injunctive relief, expenses, and attorney's fees.

MOFO CONTACTS

Kristen J. Mathews
Partner, New York
(212) 336-4038
KMathews@mofo.com

Julie O'Neill
Partner, Boston
(617) 648-4731
JOneill@mofo.com

Purvi G. Patel
Partner, Los Angeles
(213) 892-5296
PPatel@mofo.com

Mary Race
Of Counsel, Palo Alto
(650) 813-5609
MRace@mofo.com

Nathan D. Taylor
Partner, Washington, D.C.
(202) 778-1644
NDTaylor@mofo.com

Marian Waldmann Agarwal
Of Counsel, New York
(212) 336-4230
MWaldmann@mofo.com

The VCDPA will become **operative on January 1, 2023.** Visit MoFo's CCPA/CPRA Resource Center for additional state privacy law resources.

Please contact

NATHAN TAYLOR
Partner | Morrison & Foerster LLP
2100 L Street, NW, Suite 900 | Washington, DC 20037
P: +1 (202) 778-1644

If you have any questions.

EXHIBIT 4

	CCPA	GDPR	VCDPA	Comparison

	CCPA	GDPR	VCDPA	Comparison
Who is Regulated?	Any for-profit entity doing business in California, that meets one of the following thresholds: • Gross revenue greater than $25 million (inflation adjusted). • Annually buys, receives, sells, or shares personal information of more than 50,000 consumers, households, or devices for commercial purposes. • Derives 50 percent or more of its annual revenues from selling consumers' personal information. The law also applies to any entity that both: • Controls or is controlled by a covered business. • Shares common branding with a covered business, such as a shared name, service mark, or trademark. Parts of the CCPA apply specifically to: • Service providers. • Third parties.	**Controllers** and **processors:** • That process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU. • Not established in the EU that process EU data subjects' personal data in connection with offering goods or services to EU data subjects, or monitoring their behavior that takes place in the EU.	For-profit entities that conduct business in Virginia or offer products or services targeted to residents in Virginia and: • Control or process the data of at least 100,000 consumers or • Control or process the data of at least 25,000 consumers and derive more than 50% of revenue from the sale of personal data.	The GDPR and CCPA's scope and territorial reach are much broader than the VCDPA. The VCDPA is more targeted toward regulating larger firms than the GDPR's processing requirement.
Who is Protected?	Consumers, defined as California residents that are either: • In California for	Data subjects, defined as identified or identifiable persons to which personal data relates.	Consumers, defined as a natural person who is a Virginia resident acting in an individual or household context. However, acting in a	The VCDPA closely parallels the CCPA in terms of protections granted. However, the VCDPA is the narrowest of the three

	CCPA	GDPR	VCDPA	Comparison
	other than a temporary or transitory purpose. • Domiciled in California but currently outside the State for a temporary or transitory purpose.		commercial or employee context is specifically excluded from the definition.	as it excludes individuals acting in the commercial and employee contexts. Each law focuses on information that relates to an identifiable natural person, however the definitions differ. Each have potential extraterritorial effects that businesses located outside the jurisdiction must consider.
What Information is Protected?	Personal information is any information that directly or indirectly: • Identifies, relates to, or describes a particular consumer or household. • Is reasonably capable of being associated with or could reasonably be linked, to a particular consumer or household. The statutory definition includes a list of specific personal information categories. Personal information does not include: • Information lawfully made available from government records. • Deidentified or aggregate consumer information. The CCPA also contains certain sector-specific exclusions for personal information covered by other legislation.	Personal data is any information relating to an identified or identifiable data subject. The GDPR prohibits processing of defined special categories of personal data unless a lawful justification for processing applies.	Personal data is any information that is linked or reasonably linked to an identified or identifiable natural person. It does not include deidentified data or publicly available information (a separately defined term). Sensitive data means a category of personal data that includes data revealing racial or ethnic origin, religious beliefs, physical or mental health diagnosis, sexual orientation, or citizen or immigrant status, as well as processing of genetic or biometric data for identification, precise geolocation data, and personal data collected from a known child. Under the VCDPA, consent is required to process this “sensitive data.”	The VCDPA is closest to the CCPA in terms of information protection. The VCDPA’s protections is a balance of both the CCPA and GDPR as the law provides protection for sensitive data (like the GDPR), but also allows for processing of publicly identifiable information (like the CCPA).

	CCPA	GDPR	VCDPA	Comparison
	The 2019 CCPA Amendments and CPRA temporarily exclude certain employee and business-to-business (B2B) personal information from most CCPA requirements until January 1, 2023.			
Anonymous, Deidentified, Pseudonymous, or Aggregated Data	Deidentified or aggregated data is not considered personal information. However, the CCPA establishes a high bar for claiming data is deidentified or aggregated and sets specific requirements for deidentifying patient information. Pseudonymous data may qualify as personal information under the CCPA because it remains capable of being associated with a particular consumer or household. However, the statute does not clearly include or exclude it.	Anonymous data is not considered personal data. While the GDPR does not mention deidentified data, the CCPA definition is similar to GDPR's concept of anonymous data. Pseudonymous data is considered personal data.	The VCDPA's definition of persona data explicitly excludes "de-identified data or publicly available information," but makes no mention of pseudonymous information.	The VCDPA, like the CCPA and GDPR does not classify deidentified information as personal information. However, the VCDPA, unlike the CCPA's pseudonymization definitions, does not require technical controls to prevent reidentification of deidentified or pseudonymous information to qualify.
Privacy Notice / Information Right	Before or at collection, businesses must inform consumers about: • The personal information categories collected. • The intended use purposes for the categories. • If the business sells personal information, a link to or online location for its Do Not Sell My Personal Information notice. • A link to or online location for the business's privacy	Controllers must provide detailed information about its personal data collection and data processing activities. The notice must include specific information depending on whether the data is collected directly from the data subject or a third party.	The VCDPA does not expressly require businesses to display a privacy notice at or before the point of the collection of personal data, nor does it require businesses to provide a "do not sell my information" link. However, a reasonable notice requirement can be derived from the requirements of Virginia Code Section 59.1-574(C). Under this Section, controllers are required to provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes (1) the categories of	Similar to the disclosure requirements of the CCPA and GDPR, the VCDPA requires businesses to display a privacy notice but differences in the specific information required and the delivery methods. However, this notice requirement is far less stringent than the CCPA's requirement and parallels more with the GDPR.

	CCPA	GDPR	VCDPA	Comparison
	notice. Business must also provide separate detailed privacy policies describing their practices and the consumer's CCPA rights. Third parties must give consumers explicit notice and an opportunity to opt out before re-selling personal information acquired from another business.		personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including appeal of a controller's decision; (4) categories of personal data shared with third parties; and (5) categories of third parties with whom the controller shares personal data.	
Security	The CCPA does not directly impose data security requirements. However, it does establish a private right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk.	The GDPR requires controllers and processors to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	Under the VCDPA, controllers are required to establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data. The VCDPA does not have a private right of action.	Substantially similar in statutory approach though reasonable security measures may vary according to an organization's circumstances and regulator interpretation. However, unlike the CCPA, the VDCPA does not have a private right of action.
Opt-Out Right for Personal Information Sales	Businesses must enable and comply with a consumer's request to opt-out of the sale of personal information to third parties, subject to certain defenses. Must include two opt-out submission methods, including an interactive form accessible online through a "Do Not Sell My Personal Information" or "Do Not Sell My Info" link in a clear and conspicuous location on its website or mobile application. Must not request reauthorization to sell a consumer's personal information for at least 12 months after the person opts-out, with some exception.	The GDPR does not include a specific right to opt-out of personal data sales. However, the GDPR does contain other rights a data subject may use to obtain a similar result in certain circumstances. For example, it permits data subjects, at any time, to: • Opt-out of data processing for marketing purposes. • Withdraw consent for processing activities. This allows data subjects to opt-out of third-party sales that support marketing purposes or rely on consent for their legal processing basis.	The VCDPA provides a Right to Opt Out of targeted advertising, the sale of personal data or profiling.	The VCDPA splits the difference between the CCPA and the GDPR offering a specified Right to Opt Out in certain circumstances as opposed to the across-the-board requirements of the CCPA.

	CCPA	GDPR	VCDPA	Comparison
Children	The CCPA prohibits selling personal information of a consumer under age 16 without consent. Children aged 13 to 15 can directly provide consent. Children under 13 require parental consent. Must establish processes verifying consent. Importantly, protections provided by the federal **Children's Online Privacy Protection Act** (COPPA) still apply on top of the CCPA's requirements.	The GDPR's default age for consent is 16, although individual member state law may lower the age to no lower than 13. The person with parental responsibility must provide consent for children under the consent age. Children must receive an age appropriate privacy notice. Children's personal data is subject to heightened security requirements.	Sensitive data is provided greater protection and includes personal data collected from children. Businesses that comply with verifiable parental consent requirements under the Children's Online Privacy Protection Act are deemed compliant with the CDPA obligations to obtain parental consent.	Substantially different requirements, other than ages involved. The CCPA only requires parental consent for personal data sales, while GDPR's parental consent requirement applies to all processing consent requests. The VCDPA relies on requirements under the Children's Online Privacy Protection Act…therefore it does not have a certain age standards in and of itself like the CCPA. The COPPA sets most of its requirement benchmarks at age 13.
Right of Disclosure or Access	Consumers have a right to request disclosure of their personal information, including household level data, and to receive additional details regarding the personal information a business collects and its use purposes, including any third parties with which it shares information. The CCPA Regulations refer to this right as the right to know, and prescribe specific procedures for businesses to follow when handling these requests.	Data subjects have a right to access their personal data, including receiving a copy and to obtain certain information about the controller's processing.	Generally similar to the others. The VCDPA does require businesses to enable consumers to opt out from sales of data to third parties. Otherwise, similar provisions exist to allow consumers to see what is disclosed and	Broadly similar rights of disclosure/access. The CCPA's right is only to obtain a written disclosure of the information. The GDPR allows broader access, which is not limited to a written disclosure in a portable format.
Right of Data Portability	In response to a request to know specific pieces of personal information, a business must provide personal information in a readily useable format to enable a consumer to transmit the information from one entity to another entity without	The GDPR includes a right to data portability to: • Receive a copy of the personal data in a structured, commonly used and machine-readable	Similar to CCPA. Right to obtain data provided to the controller in a portable, feasible, readily usable format that should and can be transferred without hinderance.	Broadly similar rights. The GDPR provides a specific right to request a controller to transfer their personal data to another controller.

	CCPA	GDPR	VCDPA	Comparison
	hindrance.	format. • Transmit the personal data to another controller (including directly by another controller where possible).		
Right to Deletion / Erasure (Right to Be Forgotten)	A consumer has the right to delete personal information a business maintains about them, including household level data, subject to certain exceptions. The business must also instruct its service providers to delete the data.	Data subjects have the right to request erasure of personal data under six circumstances (the right to be forgotten). Controllers must also take reasonable steps to inform any other controllers also processing the personal data.	Right to delete personal data obtained by consumer exists. Some exceptions, as required by law, do exist, so similar to CCPA in that regard	Similar data deletion rights. The GDPR right only applies if the request meets one of six specific conditions. By contrast, the CCPA right is broad, but also provides broader justifications to deny requests and retain data. The GDPR's obligation to inform downstream data recipients of the person's deletion request is also broader.
Right of Rectification	None.	The GDPR grants data subjects the right to: • Correct inaccurate personal data. • Complete incomplete personal data.	Right to rectify or correct inaccuracies does exist, unlike the CA law.	Substantially different. VCDPA Closer to the GDPR on this point.
Right to Restrict Processing	None, other than the right to opt-out of personal information sales.	Right to restrict personal data processing under certain circumstances.	Can opt out of profiling and processing for targeted advertising. This can relate to a person's economic situation, identity, gender, interests, location, etc. More akin to GDPR.	Substantially different. VCDPA grants some rights here.
Right to Object to Processing	None, other than the right to opt-out of personal information sales.	Right to object to processing for profiling, direct marketing, statistical, scientific, or historical research purposes.	Can opt out of profiling and processing for targeted advertising. This can relate to a person's economic situation, identity, gender, interests, location, etc. Specifically with profiling, rights include: "…To opt out of the	Substantially different.

	CCPA	GDPR	VCDPA	Comparison
			processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant	
Non-Discrimination	A business must not discriminate against a consumer because they exercised their rights. However, a business may charge differently if that difference directly and reasonably relates to the business value provided by the consumer's data. Businesses may also offer financial incentives if they are disclosed in terms or online privacy policy, and require opt-in consent. The CCPA Regulations contain illustrative examples of discriminatory and non-discriminatory practices, and list factors businesses must consider when calculating the value of consumer data.	It is implicit in the GDPR that organizations cannot discriminate against a data subject that exercises his rights, for example by references prohibiting processing that adversely affects data subjects' rights and freedoms.	Profiling and processing for purposes of VCDPA means any processing done manually or automatically. Can opt out from profiling "in furtherance of decisions that produce legal or similarly significant effects on the consumer." May appear more narrow just based on language, but no mechanical differences between this and CCPA.	Similar idea, different obligations.
Responding to Rights Requests	A business must: • Confirm receipt of the request in writing within 10 business days. • Comply with a verifiable consumer request. • Respond within 45 calendar days after receipt, potentially extendable once for another 45 calendar days on customer notification. • Inform the	A controller must: • Verify the data subject's identity before responding to a request. • Respond to requests without undue delay and at the latest within one month, extendable for up to two more months if necessary after data subject notice. • Give reasons if the controller does not comply with any requests. Requests do not have to	A controller must • Respond within 45 calendar days after receipt, potentially extendable once for another 45 calendar days on customer notification provided additional requirements are met • Controllers are required to provide information in response to a consumer request	All three laws require substantially similar responses to request from consumers. The VCDPA is practically a mirror image of the California law.

	CCPA	GDPR	VCDPA	Comparison
	consumer of the reasons for not taking action. • Provide the information free of charge, unless the request is manifestly unfounded or excessive. Consumers may only make most information requests twice a year and only for a 12-month look-back. There are no limits on deletion and do not sell requests.	be free to data subjects.	free of charge, up to twice annually per consumer. • The controller may charge the consumer a reasonable fee or decline to act on the request if requests are manifestly unfounded, excessive or repetitive, but the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request is on the controller. Justification for failure to act. Section 59.1-573(B)(2). If a controller declines to act regarding the consumer's request, the controller shall inform the consumer why within 45 days and provide instructions for how to appeal the decision.	
Penalties (Private Rights of Action)	The CCPA establishes a narrow private right of action for certain data breaches involving a sub-set of personal information. However, the CPPA grants companies a 30-day period to cure violations, if possible. Consumers may seek the greater of actual damages or statutory damages ranging from $100 to $750 per consumer per incident. Courts may also impose injunctive or declaratory relief.	The GDPR establishes a private right of action for material or non-material damage caused by a controller or processor GDPR breach.	No private cause of action. Enforcement only by the attorney general. The attorney general has investigative authority and exclusive authority to enforce violations of the VCDPA. Prior to initiating any action, the attorney general is required to provide the controller or processor a 30-day period to cure the alleged violation. If the controller or processor fails to cure the alleged violation, the attorney general may initiate an action and seek an injunction and civil	The GDPR provides very broad consumer rights The CCPA establishes a narrow private right for certain data breaches. The VCDPA provides no private right.

	CCPA	GDPR	VCDPA	Comparison
			penalties of up to $7,500 for each violation. The attorney general may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees.	
Penalties (Civil Fines)	The California AG may bring actions for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional. However, the CCPA also grants businesses a 30-day cure period for noticed violations.	Administrative fines can reach EUR20 million or 4% of annual global revenue, whichever is highest. EU member states can impose their own penalties for GDPR infringements that are not subject to administrative fines under Article 83, GDPR.	The Virginia Attorney General may initiate an action and seek an injunction and civil penalties of up to $7,500 for each violation. Prior to any action, the AG shall provide a 30-day notice to cure. The attorney general may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees.	Approach to calculating fines differs, but violations may potentially result in significant economic liability. Virginia penalties are higher than California penalties, except for intentional violations.

EXHIBIT 5

GEORGE MASON UNIVERSITY ANTONIN SCALIA LAW SCHOOL
LAW & ECONOMICS CENTER

Private Litigation Under the California Consumer Privacy Act

CCPA REPORT | MAY 2021

ABOUT US

Because laws are incentives for changing behavior and achieving policy objectives, it is vital that the policymakers who create and shape our laws understand economic concepts and methods.

Since its inception in 1974, the Law & Economics Center has played a critical role as a leader in law and economics research and education. The LEC recognizes both the importance of timely, relevant, and unassailable research on public policy issues as well as the necessity of communicating research findings to those who are directly shaping our country's public policy discussions. With research divisions devoted to top-quality legal policy analysis and educational arms reaching out to judges, attorneys general, and other policymakers, the LEC is uniquely equipped to positively affect national policy outcomes.

The generous support of individuals, foundations, and corporations makes all LEC activities possible. A current list of LEC donors may be found on our website at www.masonlec.org

The mission of the Program on Economics & Privacy (PEP) is to promote the sound application of economic analysis to issues surrounding the digital information economy through original research, policy outreach, and education. The PEP is dedicated to studying the economic tradeoffs inherent to privacy, data security, and other digital information debates, and to produce relevant and original research and education programs for policymakers.

Acknowledgements

James C. Cooper was the principal investigator for this report. Rachel Burke, Sydney Dominguez, Jacob Hopkins, Andrew Mercado, and Peter van Ness provided outstanding research assistance in the preparation of this report.

Private Litigation Under the California Consumer Privacy Act

A REPORT BY

Program on Economics & Privacy
Law & Economics Center
George Mason University, Antonin Scalia Law School

TABLE OF CONTENTS

INTRODUCTION & EXECUTIVE SUMMARY

In June of 2018, the Governor of California signed the California Consumer Privacy Act (CCPA) into law. The law went into effect on January 1, 2020, and the Attorney General promulgated regulations to implement the CCPA in August 2020. Broadly, the CCPA is designed to protect consumer privacy by providing transparency into the personal data that businesses collect and share, and giving consumers the right to prevent companies from sharing their data with third parties.

Although these core privacy provisions are enforced exclusively by the California Attorney General, the CCPA provides a private right of action when a business's failure to implement "reasonable security practices and procedures" results in the theft of personal information.[1] In this Report, we examine the private actions filed under the CCPA since its effective date. Key findings include:

- As of March 30, 2021, 83 actions have been filed under the CCPA, with 41% actions filed or transferred into the Nortern District of California.
- 59% of the cases in our sample include at least two claims arising from the same alleged CCPA violation, and 77% of the cases in the sample use the same alleged violation of the CCPA as a predicate for either negligence or unfair competition law (UCL) claims.
- Over half (54%) of the cases are filed against the same 11 defendants.
- While the majority of cases are filed under the CCPA's data breach provisions, plaintiffs have filed a surprisingly large number of actions (19) alleging violations of the notice and choice provisions, either directly or as a predicate for a UCL claim.
- Currently, 66 cases are pending and 17 cases have settled or have been voluntarily dismissed.
- Only one court has yet to address CCPA claims on a motion to dismiss.

[1] CAL. BUS. & PROF. CODE § 1798.150(a)(1).

OVERVIEW OF THE CCPA

The core of the CCPA is a robust notice and choice regime for consumers.[2] Specifically, the CCPA requires covered businesses to notify consumers, before or at the time of collection, what "personal information" the business collects, for what purpose and how long the business intends to retain each kind of information.[3] Perhaps the most well-known provision in the CCPA requires notice to consumers if their personal information is shared with third parties, and a visible option to stop this sharing through the "Do Not Sell My Personal Information" link.[4] Further, regulations updated in March 2021 established that a business that sells personal information collected offline (e.g. at a brick-and-mortar location) must also inform consumers by an offline method of their right to opt-out.[5]

The CCPA has a broad definition of personal information, covering anything from names, to contact information, usernames, commercial records, internet history, employment or educational history, and geographic details.[6] Importantly, personal information for the CCPA's data breach provisions, which are enforceable through a private right of action, relies on the narrower definition found in the California Consumer's Records Act (CCRA).[7] Under the CCPA, businesses cannot collect or use any infor-

2 CAL. BUS. & PROF. CODE § 1798.100(b)(e); § 1798.140(c). A business meeting any of the following criteria must meet CCPA provisions: Earns more than $25 million in annual revenue; exchanges personal information from at least 50,000 consumers, devices or households; derives at least 50% of its revenue from selling consumers' personal information; or owns or is owned by a company meeting one of the above.

3 § 1798.100(b)-(e); § 1798.110(d).

4 § 1798.120(a)-(b).

5 CAL. CODE REGS. TIT. 11, § 999.306(b)(3) (effective Mar. 15, 2021)

6 § 1798.100(b)-(e); § 1798.140(o) defines personal information as anything "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This includes 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, categories of personal information described in subdivision (e) of Section 1798.80, characteristics of protected classifications under California or federal law, commercial information (including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies), biometric information, 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 website, application, or advertisement), geolocation data, audio, electronic, visual, thermal, olfactory, or similar information, employment information, education information (defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act), or inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

7 CAL. CIV. CODE § 1798.81.5. The CCRA defines personal information as "unencrypted or unredacted" first and last names plus social security numbers, government issued ID numbers, or financial account numbers along with required access codes. Id.

mation for purposes beyond what they specify in their notice to consumers.[8] The CCPA gives consumers a right to request that a business inform them which data it has collected about them in particular, how it was collected, for what purpose, and with what types of third parties the business may have shared the information.[9] The CCPA also provides consumers deletion rights.[10] Deidentification, complete erasure, or aggregation of the data can satisfy the deletion requirements.[11]

The Act seeks to prevent retaliation as a result of a consumer's request pertaining to the CCPA by prohibiting businesses from treating the consumer differently in terms of price, quality, and product availability based on an opt out.[12] However, businesses may offer incentives for consumers to allow collection of personal data, with compliant notice from businesses and consent from consumers.[13] If a business offers compensation for use of consumers' personal information, it must describe its means of determining the value of the incentive,[14] and the business must consider a designated range of valuation methods, including the marginal, average, and aggregate values associated with data collection, sale, or deletion.[15]

Enforcement

The California Attorney General is authorized to enforce the CCPA,[16] and the CCPA specifically provides that nothing in it serves as the basis for a private right of action under any other law.[17] The CCPA does provide a private right of action related to data breaches. Specifically, if a consumer's personal information is subject to "unauthorized access" as a result of "a business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information," the consumer may pursue civil action to seek damages or other relief.[18] Before commencing such action, the plaintiff must notify the defendant, who has 30 days to cure.[19] As noted above, the definition of personal information for purposes of the CCPA's private right of action comes from the CCRA, which is narrower than the CCPA's broad definition of personal information.

PRIVATE LITIGATION UNDER THE CCPA

Although the California Attorney General's Office promulgated CCPA regulations in August 2020, it has yet to bring an enforcement action.[20] Private litigation under the CCPA, however, has been active since the beginning of 2020, when the law became effective. A search of federal and state civil dockets for private actions filed from January 1, 2020 through March 30, 2021 that included claims for some violation of the CCPA resulted in a sample of 83 cases, all but one which were filed as class actions. We provide more details about these cases below.[21]

Timing and Venue

Figure 1 shows the timing of case filings. The first cases were filed at the beginning of February 2020, which would suggest that these early plaintiffs sent the thirty-day notice that must be provided to defendants before a suit can commence around January 1, 2020—the first effective day of the CCPA. The spikes in filings typically coincide with a rash of actions against a particular defendant. For example, all of the cases against Bank of America were filed between January 14, 2021 and March 26, 2021, and similarly, all of the cases against Zoom were filed between March 31, 2020 and May 13, 2020. Filings appear to slow down in August and December, coinciding with summer vacation and major holidays.

[8] § 1798.100(b).
[9] § 1798.100(a); § 1798.110(a).
[10] § 1798.105(b).
[11] CAL. CODE REGS. TIT. 11, § 999.313(d)(2).
[12] See § 1798.125(a)(1).
[13] § 1798.125(a)(2), (b).
[14] § 999.307(b).
[15] § 999.337(a).
[16] § 1798.155(b). Businesses are considered out of compliance with the CCPA if violations are not rectified within 30 days of notification, at which point fines up to $2,500 for unintentional violations and $7,500 for intentional violations are possible. Id.
[17] § 1798.150(c). Through § 1798.192, the law does not allow agreed upon deviation from its directives, rendering any portion of contracts attempting to waive the enactments of the title void.
[18] § 1798.150(a)-(b). The CCPA provides that a consumer can recover actual damages, or a minimum of $100 and a maximum of $750 per incident, whichever is greater. § 1798.150(a)(1)(A).
[19] § 1798.150(b).
[20] See Office of California Attorney General, Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act (March 15, 2021) (noting that "Since CCPA enforcement began on July 1, 2020, the Department has seen widespread compliance by companies doing business in California, especially in response to notices to cure"), at https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data.
[21] Research was performed on the Dockets database on Bloomberg Law. The search terms were "California Consumer Privacy Act," "CCPA," "1798.100," and "1798.150." Cases in which an amended complaint removed CCPA claims prior to the defendant filing a motion to dismiss are not included, although cases in which a plaintiff removes CCPA claims after the defendant files a motion to dismiss are included. We include four cases that had CCPA claims when filed, but were subsequently consolidated with other cases, and the consolidated complaint lacked a CCPA claim. Further, cases originally filed in state court, but removed to federal district court are counted as federal cases, although the original filing date in state court is retained as the filing date.

FIGURE 1
TIMING OF CCPA CASE FILINGS

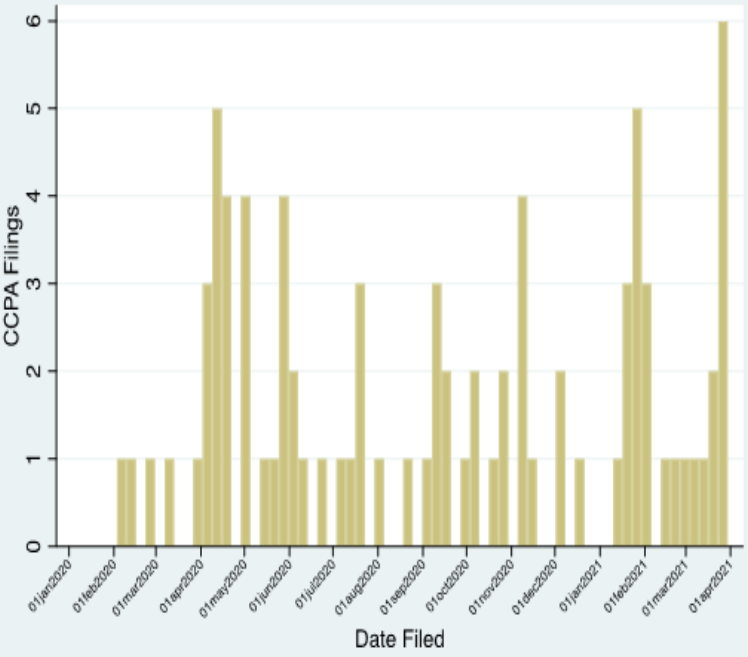


FIGURE 2
CASES BY COURT

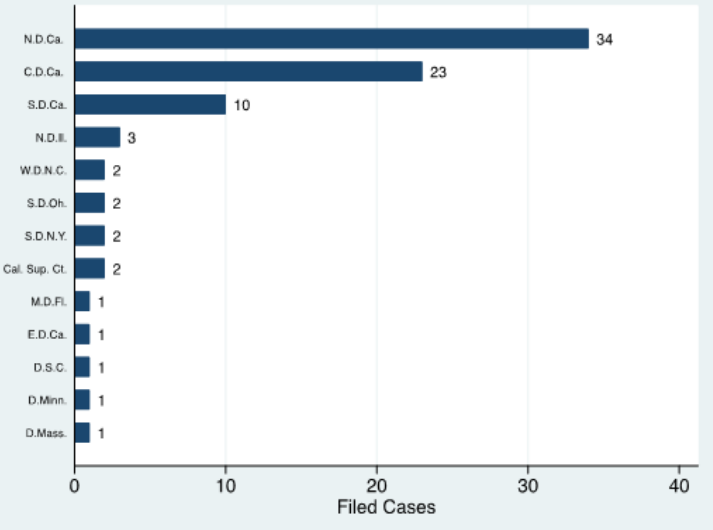


Figure 2 shows the venue for filed cases. Although CCPA cases have been filed in 13 separate courts, not surprisingly, the vast majority (84%) of cases were filed in California, with nearly half of the sample filed—or transferred to—the Northern District of California. Although seven cases were originally filed in California Superior Court, only two remain—defendants used the Class Action Fairness Act (CAFA) to remove the other five cases to federal court.[22] The Northern District of Illinois has the most CCPA cases for a non-California Court, with all of these cases involving allegations that Clearview violated the Illinois Biometric Privacy Protection Act in addition to the CCPA.

Although our search found 83 separate CCPA actions, there are only 50 separate defendants. As Table 1 shows, over half (45) of the cases were filed by separate plaintiffs against the same 11 defendants for the same (or similar) alleged conduct. For example, plaintiffs have filled 14 consumer class actions cases against Bank of America, and 10 against Zoom, which together account for 29 percent of the private CCPA actions in the database.

TABLE 1
DEFENDANTS WITH MULTIPLE CCPA ACTIONS

Defendant	Number of Cases with CCPA Allegations	Courts
Bank of America	14	N.D. Cal.* S.D. Cal. C.D. Cal.
Zoom	10**	N.D.Cal.* C.D. Cal.
Blackbaud	3	C.D. Cal. D. S.C.*
Clearview	3	N.D. Il* S.D.N.Y.
Automatic Funds Transfer Service	3	C.D. Cal.
Plaid	2	N.D. Cal.
Luxottica	2	S.D. Oh.
Tandem Diabetes Care	2	S.D. Cal.
Dickey's Barbecue Restaurants	2	S.D. Cal.
Accellion	2	N.D. Cal.
Radnet	2	C.D. Cal.

*District court where cases are being consolidated.

**3 of the originally-filed Zoom class actions complaints with CCPA claims were later merged into the consolidated class complaint, which did not include CCPA claims. Plaintiffs in the remaining 7 cases either voluntarily dismissed their claims or otherwise were not listed as plaintiffs in the consolidated complaint.

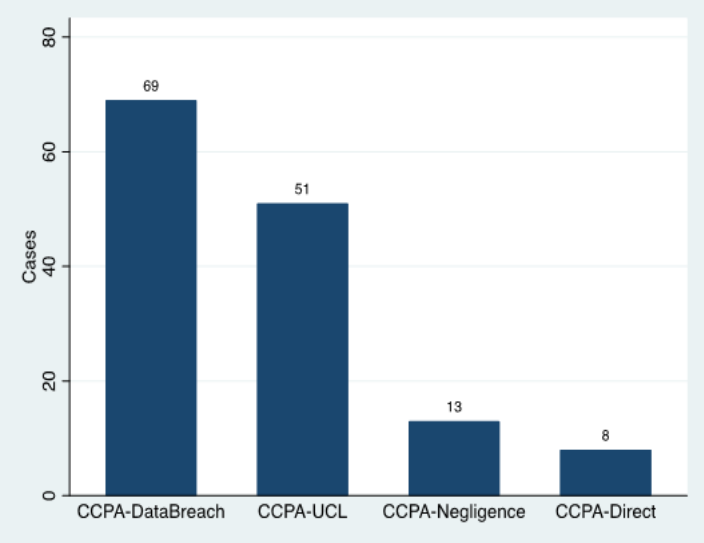
[22] The Class Action Fairness Act allows a defendant to remove a class action to federal court under certain circumstances. 28 U.S.C. § 1332(d). See Emery G. Lee, III & Thomas E. Willging, The Impact of the Class Action Fairness Act on the Federal Courts: An Empirical Analysis of Filings and Removals, 156 U. PENN. L. REV. 1723 (2008) (finding an increase in tort and state CPA class actions filed in, or removed to, federal courts after CAFA).

Types of CCPA Claims

Although the CCPA only allows a narrow private right of action based on data breach, plaintiffs have been creative in their pleading, incorporating CCPA violations into their cases through common law negligence and California's unfair competition law (UCL). Indeed, 49 (59%) of the cases include multiple claims for relief related to the same alleged CCPA violation.

Figure 3 shows the number of cases that contain the different types of CCPA claims plaintiffs include in their complaints. Data breach claims under §1798.150 are the majority of private actions, appearing in 69 (83%) of cases, but UCL claims predicated on violations of the CCPA are also found in 51 (61%) of cases, and 13 cases (16%) allege negligence based on a CCPA violation. The data show that 40 (48%) of the cases alleging a §1798.150 violation also plead the alleged CCPA violation as a predicate for a UCL violation. Further, 10 (12%) cases allege the practices violating §1798.150 constitute UCL violations and negligence.

FIGURE 3
CCPA CLAIMS FOR RELIEF



Some plaintiffs have brought claims directly under the core privacy provisions of the CCPA, which are not subject to the private right of action. For example, in *Henry v. Zoom*, the plaintiffs allege that Zoom violated § 1798.100(b) "by using customers' information without providing the required notice . . . that it was disclosing their information to unauthorized parties," and violated §1798.120(b) by failing to provide plaintiffs "the opportunity to opt out before it provided their information to unauthorized parties."[23] As shown in Figure 3, however, this strategy is rare: with only 8 cases directly alleging a violation of some provision of the CCPA other than §1798.150. Nonetheless, though plaintiffs appear hesitant to plead a direct violation of the non-data breach provisions of the CCPA, alleged violations of these provisions form the basis for nearly a quarter (23%) of all UCL claims.

Status

Given the length of class action litigation, most of these cases are still pending and none have been certified. As Table 2 illustrates, only 17 cases have settled or have been voluntarily dismissed by the plaintiff. Defendants have filed motions to dismiss in 13 cases. Theories for dismissal of the claims based on the CCPA have included:

- The consumer data at issue does not qualify as "personal information" under the statutory definition.[24]
- Insufficient allegations to support a plausible inference that the defendant's security practices were unreasonable.[25]
- The defendant is not a California resident, and thus lacks standing to assert a CCPA claim.[26]
- The defendants are "service providers," not "businesses," and thus not covered by §1798.150's provisions.[27]
- Insufficient allegations to support a plausible inference that data were "exfiltrated," as required by the statute.[28]
- The CCPA expressly precludes UCL claims predicated on a CCPA violation.[29]
- The defendant cured the alleged violation after notice.[30]

[23] Complaint at ¶¶97-98, Henry v. Zoom, No. 5:20-cv-02691-SVK (N.D. Cal. 2020). These claims were not included in the consolidated class action. See In re Zoom Communications Privacy Litigation, No. 5:20-cv-02155-LHK (N.D. Cal. Apr. 17, 2020).
[24] Memorandum in Support of Defendant's Motion to Dismiss at 5, Gardiner v. Walmart Inc., No. 20-cv-4618, (N.D. Cal. Dec. 14, 2020).
[25] Memorandum in Support of Defendant's Motion to Dismiss at 21-22, Burns v. Mammoth Media, Inc., No. 2:20-cv-04855-DDP-SK (C.D. Cal. Sept. 14, 2020).
[26] See id.
[27] Memorandum in Support of Defendant's Motion to Dismiss at 9-10, Karter v. Epid Systems, Inc., No 8:20-cv-01385-CJC-KES (C.D. Cal. Sept. 4, 2020).
[28] Id. at 13-14.
[29] Memorandum in Support of Defendant's Motion to Dismiss at 11-12, McCreary v. Filters Fast, L.L.C., No. 3:20-cv-595-FDW-DCK (W.D.N.C. Jan. 29,2021).
[30] Id. at 12-13.

TABLE 2
CASE STATUS

All Cases		Motion to Dismiss Filed		
Pending	Settled or Voluntarily Dismissed	Decided	Settled or Voluntarily Dismissed Before Decided	Pending
66	17	4	3	6

Although 4 motions to dismiss have been decided in our sample, only one court actually had to address the CCPA: plaintiffs appear to have voluntarily dismissed their CCPA claims after the defendant filed their motion to dismiss in two cases;[31] and the district court decided against the plaintiff on standing grounds in the other.[32]

Gardiner v. Walmart is the only case in our database in which the court directly addressed a CCPA allegation on a motion to dismiss.[33] In Gardiner, the plaintiff alleged, *inter alia*, that he suffered harm under §1798.150 because a data breach involving Walmart led to his personal information being available for sale on the "dark web."[34] The district court held that Gardiner had failed to state a claim for two reasons. First, he failed to allege that the breach occurred after January 1, 2020, the date the CCPA went into effect.[35] Finding data on the dark web after January 1, 2020, was insufficient to support his claim, because the alleged unreasonable security practices that led to the breach of data must have taken place after January 1, 2020.[36] Second, Gardiner failed to plead that the information in question qualifies as "personal information," under the CCPA's data breach provisions, which key on the CCRA's narrower definition. Although he generally alleged that the breach compromised "full names, financial account information, credit card information, and other PII of Walmart customers," the court held that the failure to allege the specific information the CCRA requires—account numbers and the required security or access codes to access the accounts—was fatal.[37] The court also held that Gardiner could not premise his UCL claim on the dismissed CCPA claim.[38]

[31] Flores-Mendez v. Zoosk, Inc., No. 3:20-cv-04929, 2021 WL 308543, (N.D. Cal. Jan. 30, 2021); Shay v. Apple Inc., No. 3:20-cv-01629, 2021 WL 75690 (S.D. Cal. Jan. 8, 2021).
[32] Rahman v. Marriott Int'l, Inc., No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021). Currently on appeal to the Ninth Circuit. See Rahman v. Marriott Int'l, Inc., No. 21-55112 (9th Cir. Feb. 12, 2021).
[33] Gardiner v. Walmart Inc., No. 20-cv-4618, (N.D. Cal. Jul. 10, 2020).
[34] Order Granting Defendant's Motion to Dismiss at 1-2, Gardiner v. Walmart Inc., No. 20-cv-4618 (N.D. Cal. Mar. 5, 2021).
[35] Id. at 2-3.
[36] Id. at 3.
[37] Id. at 5.
[38] Id. at 13.

CONCLUSION

In the sixteen months since the CCPA went into effect, plaintiffs have filed 83 cases alleging some violation of the CCPA, over half of which were filed against the same 11 defendants. Most of the cases allege violations of Section 1798.150 (directly, and as predicates for UCL and negligence claims), the provision of the CCPA that provides a private right action for data breaches that result in the theft of personal information. A non-trivial number of plaintiffs, however, have alleged claims based on the core privacy provisions of the CCPA, either directly or as predicates for UCL violations. So far, only one court has had the opportunity to weigh on the CCPA, ultimately dismissing the CCPA claims. Several other courts, however, soon will have the opportunity to help further clarify the metes and bounds of the private right of action under the CCPA.

:ORGE MASON UNIVERSITY ANTONIN SCALIA LAW SCHOOL

LAW & ECONOMICS CENTER

3301 Fairfax Drive
Arlington, VA 22201
P 703.993.8040 **F** 703.993.8181
www.MasonLEC.org
@MasonLEC @MasonLEC
Law & Economics Center

EXHIBIT 6

2021 WL 2520103
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

Lavarious GARDINER, Plaintiff,
v.
WALMART INC., Defendant.

Case No. 20-cv-04618-JSW
|
Signed 03/05/2021

Attorneys and Law Firms

Bobby Saadian, Justin F. Marquez, Robert James Dart, Thiago Merlini Coelho, Wilshire Law Firm, PLC, Los Angeles, CA, for Plaintiff.

Ann Marie Mortimer, Jason Jonathan Kim, Jeff R. R. Nelson, Hunton Andrews Kurth LLP, Robert James Herrington, Greenberg Traurig LLP, Los Angeles, CA, for Defendant.

ORDER GRANTING MOTION TO DISMISS AND DENYING MOTION TO STRIKE CLASS ALLEGATIONS

Re: Dkt. Nos. 35, 36

JEFFREY S. WHITE, United States District Judge

***1** Now before the Court for consideration is the motion to dismiss and motion to strike class allegations filed by Defendant Walmart Inc., ("Walmart" or "Defendant"). The Court has reviewed the parties' papers, relevant legal authority, and the record in this case, and it finds this matter suitable for disposition without oral argument. *See* N.D. Civ. L.R. 7-1(b). For the following reasons, the Court GRANTS Walmart's motion to dismiss and DENIES Walmart's motion to strike.

BACKGROUND

Walmart is a retailer selling goods in its stores and online via its website. (Dkt. No. 1, Complaint ("Compl.") ¶¶ 1, 14.) Plaintiff Lavarious Gardiner alleges that he provided certain personal identifying information ("PII") to Walmart when creating his online account. (*Id.* ¶ 7.) Plaintiff alleges that the PII customers provide to Walmart when they create an online account includes credit card information. (*Id.* ¶ 14.) Plaintiff alleges on information and belief that his PII was accessed by hackers because of a data breach that took place at Walmart. (*Id.* ¶ 7.) According to Plaintiff, hackers have targeted Walmart numerous times "by hacking Walmart's website and Walmart's customers' computers" and then posting the stolen account information on the "dark web," which "is replete with stolen Walmart accounts for sale." (*Id.* ¶¶ 14, 15.) Plaintiff alleges that his data is currently being sold on the dark web as a result of the data breach and that he has communications with hackers affirming that the accounts being sold belong to Walmart customers. (*Id.* ¶¶ 7, 15-16.)

As a result of the purported breach of Walmart's website, Plaintiff alleges that he and the proposed class face an imminent threat of identity theft and fraud. This has led them to spend time and resources mitigating the effects of the data breach, including by placing "freezes" and "alerts" with credit card agencies, closing or modifying financial accounts, and carefully monitoring their credit reports. (*Id.* ¶ 41.) Plaintiff further alleges that he and the proposed class have suffered economic damages and actual harm in the form of: (1) the improper disclosure of their PII; (2) the imminent injury flowing from potential fraud and identity theft; (3) nonexistent notification of the data breach; (4) ascertainable losses in the form of out-of-pocket expenses and value of time spent mitigating the data breach's effect; (5) losses in the form of deprivation of value of their PII; and (6) overpayments for the goods purchased from Walmart. (*Id.* ¶ 42.)

Plaintiff brings the following causes of action: (1) violations of the California Consumer Privacy Act, Cal Civ. Code § 1798.150 *et seq.* ("CCPA"); (2) negligence; (3) violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"); (4) breach of express contract; (5) breach of implied contract; and (6) breach of the implied covenant of good faith and fair dealing. Plaintiff seeks compensatory damages and injunctive relief.

The Court will address other facts as necessary in the analysis.

ANALYSIS

A. Walmart's Motion to Dismiss.

1. Legal Standard Applicable to Rule 12(b)(6).

***2** A motion to dismiss is proper under Federal Rule of Civil Procedure 12(b)(6) where the pleadings fail to state a claim upon which relief can be granted. The Court's "inquiry is limited to the allegations in the complaint, which are accepted as true and construed in the light most favorable to the plaintiff." *Lazy Y Ranch LTD v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008). Even under the liberal pleading standard of Federal Rule of Civil Procedure 8(a)(2), "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell At. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)).

Pursuant to *Twombly*, a plaintiff must not merely allege conduct that is conceivable but must instead allege "enough facts to state a claim to relief that is plausible on its face." *Id.* at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). If the allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. *See, e.g.*, *Reddy v. Litton Indus., Inc.*, 912 F.2d 291, 296 (9th Cir. 1990); *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246-47 (9th Cir. 1990).

2. Plaintiff's CCPA Claim Fails.

Walmart argues that Plaintiff's CCPA claim fails for two reasons: (1) Plaintiff's failure to allege when the breach occurred is fatal to the CCPA claim because the statute only applies to breaches occurring after January 1, 2020; and (2) Plaintiff does not adequately allege the disclosure of personal information, as defined by the statute.

The CCPA permits "[a]ny consumer whose nonencrypted and nonredacted personal information [...] 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" to recover damages or injunctive relief. Cal. Civ. Code § 1798.150(a)(1).

The CCPA went into effect on January 1, 2020, and it does not contain an express retroactivity provision. *See* Cal. Civ. Code § 1798.198 (providing the CCPA "shall be operative January 1, 2020); *see also* Cal. Civ. Code § 3 ("[n]o part of [this Code] is retroactive, unless expressly so declared."). Moreover, it is well-settled under California law that "in the absence of an express retroactivity provision, a statute will not be applied retroactively unless it is very clear from extrinsic sources that the Legislature must have intended a retroactive application." *See, e.g.*, *People v. Brown*, 54 Cal. 4th 314, 319-20 (2012); *Aetna Cas. & Sur. Co. v. Indus. Acc. Comm'n*, 30 Cal. 2d 388, 393 (Cal. 1947). Based on the text of the statute and California law, the Court concludes that the challenged provision of the CCPA does not apply retroactively. Accordingly, the alleged breach here is only actionable under the CCPA if it occurred after January 1, 2020.

Plaintiff does not dispute that the CCPA does not apply retroactively, and he concedes that he has not alleged the specific date of the breach. (*See* Opp. at 6 ("[H]e cannot say specifically when Defendant's system was breached.").) Plaintiff argues, however, that his allegation that his personal information is currently available on the dark web satisfies his pleading obligation. The Court disagrees. In order to have a viable claim against Walmart for a violation of the CCPA, Plaintiff must allege that Walmart's "violation of the duty to implement and maintain reasonable security procedures and practices" that led to the breach occurred on or after January 1, 2020. *See* Cal. Civ. Code § 1798.150(a)(1). Plaintiff has not done so. Although Plaintiff alleges that unnamed third-party criminals are currently circulating his personal information on the dark, he does not allege that the breach of Walmart's website—the relevant conduct—occurred no earlier than January 1, 2020. Absent allegations establishing that Walmart's alleged violation of the CCPA occurred after it went into effect, Plaintiff's CCPA claim is not viable.

***3** Plaintiff's CCPA claim also fails because the complaint does not sufficiently allege disclosure of Plaintiff's personal information. "Personal information" means:

> (A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
>
> (i) Social security number.
>
> (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
>
> (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account [...]
>
> (B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

Cal. Civ. Code § 1798.81.5.

Plaintiff alleges that the purported breach compromised the full names, financial account information, credit card information, and other PII of Walmart customers. Although Plaintiff generally refers to financial information and credit card fraud, he does not allege the disclosure of a credit or debit card or account number, and the required security or access code to access the account. Plaintiff concedes that the complaint does not contain such allegations. Instead, in opposition, he asks the Court to assume that the access code for a credit card is the expiration date plus the three-digit passcode on the back of the card, both of which are included when selling credit card numbers on the dark web "[o]therwise, the numbers would be useless to criminals." (Opp. at 7.) Plaintiff also asks the Court to assume that when Plaintiff entered his credit card information into his Walmart account that included the card's expiration date and security number "[o]therwise, Walmart would not have been able to charge the card." (*Id.* at 8.) From this string of speculation, Plaintiff urges that "the [c]omplaint must be read as to allege that this security information, in addition to the card number, is available for sale on the dark web." (*Id.*) But these allegations are not in the complaint; Plaintiff raises them for the first time in opposition. Although the Court will draw reasonable inferences in Plaintiff's favor at this stage, it cannot read missing allegations into the complaint. *Johnson v. Cty. of Santa Clara*, No. 5:18-CV-06264-EJD, 2019 WL 1597488, at *3 (N.D. Cal. Apr. 15, 2019) ("[A] complaint may not be amended by briefs in opposition to a motion to dismiss.") (quoting *Barbera v. WMC Mortg. Corp.*, 2006 WL 167632, at *2 n. 4 (N.D. Cal. Jan. 19, 2006)).

Accordingly, the Court GRANTS Walmart's motion to dismiss Plaintiff's CCPA claim.

3. Plaintiff Has Not Sufficiently Alleged Injury to Support His Remaining Claims.

Walmart moves to dismiss Plaintiff's remaining claims for negligence, contract, and violations of the UCL for failure to plead cognizable injury. Plaintiff contends that he presents four theories of injury that support his claims: (1) loss of value of his PII; (2) future risk of identity theft; (3) out-of-pocket expenses for credit monitoring services; and (4) the benefit of the bargain. Specifically, Plaintiff alleges that he and the class members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, and which forced Plaintiff and the class members to adopt costly and time-consuming preventative and remediating efforts, including cancelling credit cards and freezing accounts. Plaintiff also alleges that he and class members were damaged because they overpaid for goods sold by Walmart for which they would not have paid had they known Walmart would not protect their PII. Plaintiff further alleges that he suffered injury when he lost the value of his PII, which "now that it has been exposed to hackers, is no longer worth the price that Plaintiff could have obtained for it on the market." (Compl. ¶¶ 95, 102.) The Court will address each theory of injury.

a. Loss of Value of PII.

***4** Plaintiff alleges damages in the form of deprivation of the value of his PII. Specifically, Plaintiff alleges that "there is a well-established national and international market" for his

and class members' PII, "which has a real market value." (*See id.* ¶¶ 42(e), 102.) Walmart argues that deprivation of value of PII is not a cognizable form of injury because Plaintiff has not alleged that he wants to sell his financial information to someone else.

Although the Ninth Circuit has recognized that allegations of diminished value of personal information may be sufficient to establish injury, *see* *In re Facebook Privacy Litig.*, 572 Fed. App'x 494 (9th Cir. 2014), Plaintiff's allegations of the lost value of his PII are insufficient to support this theory of damages. Plaintiff asserts that a market exists for his PII, but he has not alleged with specificity what PII was stolen. Plaintiff refers generally to compromised credit card numbers, but he concedes in his opposition that a credit card cannot be used without an access code or password and/or expiration date. He does not allege that this information was compromised, and a credit card number alone may not have significant value to cause harm. *See* *Brett v. Brooks Bros. Grp.*, No. CV 17-4309-DMG (Ex), 2018 WL 8806668, at *4 (C.D. Cal. Sept. 6, 2018) (noting that harm of future identity theft was conjectural when the personal information at issue involved only the credit card numbers and names). This sets Plaintiff's allegations apart from those in the cases he cites. *See, e.g.*, *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429, at *1 (N.D. Cal. Apr. 1, 2015) (PII shared with third party included "credit card information, purchase authorization, addresses, zip codes, names, phone numbers, email addresses, and/or other information"); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (PII allegedly exposed in data breach included names, birth dates, social security numbers, health care ID numbers, home addresses, email address, employment information, and health information including medical history and payment and billing records). Accordingly, without additional factual allegations identifying what PII was stolen, Plaintiff's bare assertions that his PII had value or that an economic market exists for Plaintiff's PII are insufficient to support his claims. *See* *Razuki v. Caliber Home Loans, Inc.*, No. CV 17-1718-LAB (WVGx), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018) (finding plaintiff failed to sufficiently allege damages to support his negligence claim where plaintiff's "claim alleging diminution of value of his personal data fails to allege enough facts to establish how his personal information is less valuable as a result of the breach.")

b. Risk of Future Harm.

Plaintiff's conclusory allegations of an increased risk of identity theft are insufficient to establish injury as required for his negligence, contract, and UCL claims. Plaintiff vaguely alleges that he and class members face an increased risk of future identity theft because hackers accessed their data, but he does not offer specific facts regarding the PII that was allegedly stolen, does not allege that any misuse has occurred, and does not allege how the stolen personal information constitutes a nonspeculative injury. "[T]he mere danger of future harm, unaccompanied by present damage, will not support a negligence action." *Huynh v. Quora, Inc.*, No. 18-cv-07597-BLF, 2020 WL 7408230, at *6 (quoting *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 951 (S.D. Cal. 2012)).

***5** Plaintiff argues that courts frequently find that an increased risk of future identity theft resulting from a data breach constitutes cognizable injury, but he relies on cases analyzing the allegations required to establish Article III injury-in-fact. *See,* *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (finding the plaintiffs sufficiently alleged "a concrete and imminent threat of future harm sufficient to establish Article III injury-in-fact at the pleading stage"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018) (risk of identity theft sufficient to allege Article III injury-in-fact); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1035 (N.D. Cal. 2019) (same); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (same).

However, the allegations required to sufficiently plead injury-in-fact for purposes of Article III standing are not the same as those required to plead damages for purposes of state law claims. *See* *Huynh*, 2020 WL 7408230, at *5 ("[T]he Ninth Circuit has held that its 'holding that Plaintiff-Appellants pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of

their state-law claims.' ") (quoting *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010)); *see also* *In re Sony Gaming*, 903 F. Supp. 2d at 963 ("While Plaintiffs have currently alleged enough to assert Article III standing to sue based on an increased risk of future harm, the Court finds such allegations insufficient to sustain a negligence claim under California law.") Indeed, Plaintiff cites cases that draw this very distinction. For example, the court in *In re Yahoo!* explained that although the plaintiffs' allegations of future injury were "sufficient to establish standing under the broader injury-in-fact requirements of Article III," the same allegations were not sufficient to allege lost money or property under the UCL. 2017 WL 3727318, at *22. The same is true here.

Walmart also argues that Plaintiff has foreclosed the possibility of future harm because the complaint alleges that he and class members have "clos[ed] or modif[ied] financial accounts" as a result of the breach. (Compl. ¶ 41.) The Court is not persuaded by Plaintiff's characterization of this allegation as a drafting error. [1] However, drawing inferences in favor of Plaintiff, the Court cannot conclude that the allegations in the complaint establish that Plaintiff has cancelled the credit cards implicated in the alleged breach. The Court cautions, however, that to the extent Plaintiff amends his complaint to clarify this allegation, he may only do so if it can be done consonant with his pleading obligations under Rule 11 of the Federal Rules of Civil Procedure. *See, e.g.*, *Volis v. Housing Auth. Of City of Los Angeles Employees Guthrie*, CV 13-01397, 2014 WL 12677316, *9 (C.D. Cal. 2014) ("[T]he Court is not required to accept as true allegations in an amended complaint that contradict an earlier complaint without explanation.").

Accordingly, Plaintiff has not sufficiently alleged a threat of future harm to sustain his negligence, breach of contract, and UCL claims.

c. Out-of-Pocket Expenses.

***6** Plaintiff also contends that he asserts a cognizable injury in the form of out-of-pocket expenses and the value of time spent attempting to mitigate the effects of the alleged data breach. Courts have found that credit monitoring may be "compensable where evidence shows that the need for future monitoring is a reasonably certain consequence of the defendant's breach of duty, and that the monitoring is reasonable and necessary." *Corona v. Sony Pictures Entm't, Inc.*, No. 14-cv-09600 RGK EX, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (citing *Potter v. Firestone Tire & Rubber Co.*, 6 Cal.4th 965, 1006-1007 (1993).)

Here, Plaintiff alleges that "as a necessary and reasonable measure to protect himself, [he] purchased a credit and personal identity monitoring service to alert him to potential misappropriation of his identity and to combat the risk of further identity theft." (Compl. ¶ 7.) Plaintiff offers no factual allegations in support of the alleged credit monitoring services, nor does he sufficiently allege that such services were reasonable and necessary. Accordingly, Plaintiff has not sufficiently alleged injury based on out-of-pocket expenses allegedly spent on credit monitoring services. *See Holly v. Alta Newport Hosp., Inc.*, No. 2:19-cv-07496-ODW (MRWx), 2020 WL 1853308, at *6 (C.D. Cal. Apr. 10, 2020) (conclusory allegations concerning mitigation or remediation insufficient where plaintiff did not provide any supporting factual allegations or allege how any credit monitoring was reasonable and necessary).

d. Benefit of the Bargain.

Plaintiff also argues that he alleges sufficient injury to support his contract and UCL claims based on a benefit of the bargain theory. Plaintiff alleges that he "suffered a monetary injury because he did not receive the benefit of his bargain with Defendants, through which he agreed to pay for goods with the understanding that his payment information would be protected by Defendants." (Compl. ¶ 94; *see also id.* ¶ 118.) Plaintiff alleges that he and class members entered into an express contract with Walmart under which they provided Walmart with their PII. According to Plaintiff, this contract incorporated Walmart's Privacy Policy. In the complaint, Plaintiff quotes portions of the Privacy Policy and provides a web address where the policy can be found. Under the Privacy Policy, Walmart represents that it uses reasonable security measures to protect a customer's personal information.

As an initial matter, Plaintiff's vague allegations do not establish how Walmart failed to take reasonable measures

to protect customer's data. In any event, Plaintiff's benefit of the bargain theory fails because he has not alleged that Walmart represented in the Privacy Policy, or otherwise, that the cost of data security was included in the cost of its goods. *See Ables v. Brooks Bros. Grp.*, No. CV 17-4309-DMG (EX), 2018 WL 8806667, at *7 (C.D. Cal. June 7, 2018) (benefit of bargain theory cognizable in data breach context in the presence of a security agreement concerning consumer data or some other representation that the cost of security is subsumed within the cost of goods). Plaintiff does not allege facts that his Walmart purchases included a sum understood by the parties to be allocated toward customer data protection nor does he allege that he was required to agree to or accept the terms of the Privacy Policy prior to engaging in any purchase. Accordingly, Plaintiff's allegations do not establish that the cost of the goods he purchased at Walmart included some amount attributable to data security as required to support his benefit of the bargain theory. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 834 (N.D. Cal. 2020) (finding benefit of bargain not a viable theory of damages where plaintiffs did not allege to have paid anything for the services); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013) (rejecting plaintiffs' benefit of the bargain theory because "the FAC fails to allege that Plaintiffs actually provided consideration for the security services which they claim were not provided"); *Huynh*, 2019 WL 11502875, at *10 (finding "lost benefit of the bargain is not sufficient to allege damages because Plaintiffs have not shown that they paid anything for the asserted privacy protections"). The Court finds this theory of injury insufficient to support his UCL and breach of contract claims.

***7** Plaintiff's vague and conclusory allegations regarding his purported injuries are insufficient to establish the damages element required for his breach of contract, negligence, and UCL claims. *See Holly*, 2020 WL 1853308, at *6 (granting motion to dismiss because plaintiff's "conclusory and vague allegations are insufficient to establish that she suffered actual damages as a result of the data breach"). Accordingly, the Court GRANTS Walmart's motion to dismiss.

4. Plaintiff's UCL Claim Is Subject to Dismissal for Other Reasons.

Walmart argues that Plaintiff's UCL claim fails for three additional reasons: (1) Plaintiff cannot show he lacks adequate remedies; (2) Plaintiff lacks statutory standing; and (3) Plaintiff cannot predicate his UCL "unlawful" claim on alleged violations of other laws.

a. Plaintiff fails to show that he lacks adequate remedies.

"Remedies under the UCL are limited to restitution and injunctive relief, and do not include damages." *Silvercrest Realty, Inc. v. Great Am. E&S Ins. Co.*, No. SACV 11-01197-CJC (ANx), 2012 WL 13028094, at *2 (C.D. Cal. Apr. 4, 2012) (citing *Korea Supply Co. v. Lockheed Martin*, 29 Cal. 4th 1134, 1146–49 (2003)). Recently in *Sonner v. Premier Nutrition Corp.*, the Ninth Circuit held the plaintiff's claims for equitable relief were properly dismissed because she failed to allege a lack of adequate legal remedy. 971 F.3d 834, 844 (9th Cir. 2020). The Ninth Circuit found "that the traditional principles governing equitable remedies in federal courts, including the requisite inadequacy of legal remedies, apply when a party requests restitution under the UCL and CLRA in a diversity action." *Id.* at 843-44. *Sonner* has been extended to claims for injunctive relief. *See, e.g.*, *Zaback v. Kellogg Sales Co.*, No. 3:20-cv-00268-BEN-MSB, 2020 WL 6381987, *4 (S.D. Cal. Oct. 29, 2020) (dismissing a UCL claim for injunctive relief because the plaintiff failed to allege that there was no adequate remedy at law); *In re Macbook Keyboard Litig.*, No. 5:18-cv-02813-EJD, 2020 WL 6047253, at *2-3 (N.D. Cal. Oct. 13, 2020) (finding that *Sonner* extends to preclude claims for injunctive relief); *Teresa Adams v. Cole Haan, LLC*, No. SACV 20-913 JVS (DFMx), 2020 WL 5648605, at *2 (C.D. Cal. Sept. 3, 2020) (finding, under the reasoning of *Sonner*, that there is no "exception for injunctions as opposed to other forms of equitable relief").

Here, Plaintiff alleges that he has suffered compensable damages, and in his opposition, he concedes that legal remedies exist. Plaintiff does not address *Sonner*, but he contends that he should be permitted to seek equitable remedies because he will have no adequate remedy at law if the Court finds his claims for legal remedies deficient. Plaintiff provides no authority in support of this position,

and the Court finds this argument unavailing. *See* *Rhynes v. Stryker Corp.*, No. 10-5619 SC, 2011 WL 2149095, at *4 (N.D. Cal. May 31, 2011) ("Where the claims pleaded by a plaintiff *may* entitle her to an adequate remedy at law, equitable relief is unavailable.")

Plaintiff also argues that he lacks adequate legal remedies because: (1) injunctive relief is required to ensure Walmart adopts industry-standard, reasonable safeguards to protect its customers; and (2) Plaintiff seeks a full refund of the purchase price of the Walmart products he purchased, which he will not receive through legal remedies. Neither argument is persuasive. First, Plaintiff has not demonstrated that the potential harm caused by Walmart's failure to protect its customers could not be remedied by monetary damages. *See* *Huynh*, 2020 WL 7495097, at *19. Second, Plaintiff would not necessarily be entitled to the full refund of the purchase price as restitution. *See* *Julian v. TTE Tech., Inc.*, No. 20-cv-02857-EMC, 2020 WL 6743912, at *5 (N.D. Cal. Nov. 17, 2020) ("[S]ome courts have held that a full refund of the purchase price is not even available as restitution.")

b. Plaintiff lacks statutory standing under the UCL.

***8** "To assert a UCL claim, a private plaintiff needs to have 'suffered injury in fact and ... lost money or property as a result of the unfair competition.' " *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) (quoting *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203 (9th Cir.2010).) Plaintiff relies on his allegations of overpayment, increased risk of identity theft, and time and money spent mitigating the risk of fraud to argue that he has established UCL standing; however, those arguments fail for the reasons discussed above. *See also* *Huynh*, 2019 WL 11502875, at *7 ("[T]hat Plaintiffs did not receive the full benefit of their bargain with Quora is not a loss of money or property because Plaintiffs did not pay for Quora's services"). Moreover, courts have widely held that "personal information" does not constitute money or property under the UCL. *See* *In re iPhone*, 2011 WL 4403963, at *14.

c. Plaintiff has not alleged a predicate violation to support his unlawful claim.

The UCL's unlawful prong allows plaintiffs to "borrow" other laws and make claims independently actionable under the UCL. *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). Here, Plaintiff's unlawful claim is premised on violations of the CCPA, CRA, and FTC. As an initial matter, Plaintiff does not meaningfully address Walmart's arguments that these violations cannot serve as the predicate for his UCL claim, and so he concedes Walmart's assertion. *Gordon v. Davenport*, No. 08-cv-3341, 2009 WL 322891, at *4 n.4 (N.D. Cal. Feb. 9, 2009). Moreover, to the extent that Plaintiff rests his unlawful claim on claims that the Court has dismissed in this order, the UCL unlawful claim must also be dismissed. *Arena Rest. & Lounge LLC v. S. Glazer's Wine & Spirits, LLC*, 2018 WL 1805516, at *13 (N.D. Cal. Apr. 16, 2018).

5. The Economic Loss Doctrine Bars Plaintiff's Negligence Claim.

Walmart argues Plaintiff's negligence claims are barred by the economic loss doctrine. Under California law, "[i]n the absence of (1) personal injury, (2) physical damage to property, (3) a 'special relationship' existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 967 (S.D. Cal. 2014) (internal citations and quotation marks omitted).

As an initial matter, the Court disagrees with Plaintiff's contention that the economic loss rule does not apply in data breach cases. Plaintiff cites out of circuit authorities for this proposition; he does not address cases in this circuit applying the economic loss rule in the data breach context, *see, e.g.*, *In re Sony Gaming*, 996 F. Supp. 2d at 972, and he cites one such case himself, which further undercuts his argument. (*See* Opp. at 21 (citing *Bass*, 394 F. Supp. 3d at 1039).)

Plaintiff argues that he has alleged non-economic harm in the form of time spent checking his credit and taking preventative measures against identity theft. However, courts have found

that the cost of lost time is an economic harm not recoverable under the economic loss doctrine. *See* *N. Am. Chem. Co. v. Superior Court*, 59 Cal. App. 4th 764, 777 n. 8 (1997) (noting that purely economic loss includes lost opportunities); *Dugas*, 2016 WL 6523428, at *12 (applying economic loss rule to negligence claims where alleged injuries included "costs associated with time spent and loss of productivity"); *In re Sony Gaming*, 903 F. Supp. 2d at 961 n.15 (S.D. Cal. 2012); *but see In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020) ("[P]laintiffs have alleged they have lost time responding to the Breach as well as suffering from increased anxiety and so do not allege purely economic losses."). Here, Plaintiff alleges that he and class members have suffered ascertainable losses in the form of "the value of their time." (Compl. ¶ 42(e).) Accordingly, the Court concludes that Plaintiff's allegations about the value of his lost time constitutes economic loss.

***9** Plaintiff also argues that even if the economic loss doctrine is applicable, a "special relationship" exists between the parties, which permits him to recover economic losses for his negligence claim. *See* *J'Aire Corp. v. Gregory*, 24 Cal.3d 799 (1979). A special relationship will exist, for example, if "the plaintiff was an intended beneficiary of a particular transaction but was harmed by the defendant's negligence in carrying it out." *Id.* Here, Plaintiff's allegations are insufficient to establish this type of special relationship. Plaintiff does not allege that the transaction at issue was intended to benefit Plaintiff in a specific way that sets him apart from all potential Walmart customers. *See* *In re Sony Gaming*, 996 F. Supp. 2d at 972. Accordingly, the Court concludes that Plaintiff's allegations fail to establish the existence of a special relationship.

6. Walmart's Limitation of Liability Clause Precludes Plaintiff's Contract Claims.

Walmart also argues that it's Terms of Use ("TOU")[2] bar Plaintiff's claims for breach of express and implied contract and breach of implied covenant of good faith and fair dealing. The TOU contains a disclaimer of warranties provision, which provides that information sent or received while using the Walmart website "may not be secure and may be intercepted or otherwise accessed by unauthorized parties." (RJN, Ex. G, § 17.) The TOU also contains a limitation of liability provision, which applies to "theft, destruction, authorized access to, alteration of, loss of use of any record or data," among other things. (*Id.*, § 18.)

"Generally, a limitation of liability clause is intended to protect the wrongdoer defendant from unlimited liability," and such clauses "have long been recognized as valid in California." *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.*, 209 Cal. App. 4th 1118, 1126 (2012) (internal quotation marks omitted). These clauses are enforceable unless unconscionable for breach of contract claims. *See id.* "[U]nconscionability has both a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided results." *Mohamed v. Uber Techs., Inc.*, 848 F.3d 1201, 1210 (9th Cir. 2016) (internal quotation marks omitted).

Plaintiff does not dispute that he agreed to the TOU, but he argues that the limitation of liability provision is both procedurally and substantively unconscionable.[3] First, Plaintiff argues that the TOU is unconscionable because it is a contract of adhesion. But adhesion contracts are not per se unconscionable under California law. *Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1261-62 (9th Cir. 2017). Second, Plaintiff contends that the TOU's limitation of liability provision creates consumer confusion because it conflicts the terms of the Privacy Policy, which renders it procedurally unconscionable. However, the limitation of liability provision contains clear language, is not buried in the TOU, and is emphasized with the use of capitalization. Accordingly, the Court concludes that the TOU put consumers on notice that Walmart's reasonable measures for protecting PII were not infallible. Plaintiff also argues that the TOU is substantively unconscionable because it "purports to waive liability for all damages of any kind...making the [TOU] completely illusory." (Opp. at 25.) Similar limitation of liability provisions, however, are routinely upheld by courts, and Plaintiff offers no contrary authority. *See, e.g.*, *Huynh*, 2019 WL 11502875, at *11 (finding similar limitation of liability provision enforceable). Accordingly, the limitation of liability provision in the TOU bars Plaintiff's contract claims. However, Plaintiff will be permitted leave to amend because facts could conceivably be alleged which would go towards determining procedural or

substantive unconscionability at the time Plaintiff entered the contract.

B. The Court Denies Walmart's Motion to Strike Class Allegations.

***10** Walmart moves to strike Plaintiff's class allegations under Rule 12(f) and under Rules 23(c)(1)(A) and 23(d)(1)(D) on the basis that innumerable unnamed class members agreed to arbitrate their claims unlike Plaintiff. Walmart argues that Plaintiff's failure to show that he is party to the arbitration agreement included in Walmart's TOU renders him an atypical and inadequate representative of the proposed class. Plaintiff seeks to represent a class of:

> All persons residing in the State of California who had a Walmart account at any time from four years prior to the date of the filing of this Complaint to the date of notice is sent to the class.

(Compl. ¶ 43.)

Rule 12(f) permits the Court, in its discretion, to "strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter." Fed. R. Civ. P. 12(f); *see also Cal. Dep't of Toxic Substance Control v. Alco Pac., Inc.*, 217 F. Supp. 2d 1028, 1033 (C.D. Cal. 2002). "Immaterial matter is that which has no essential or important relationship to the claim for relief or the defenses being pleaded." *Fantasy, Inc. v. Fogerty*, 974 F.2d 1524, 1527 (9th Cir. 1993) (internal quotations and citations omitted), *rev'd on other grounds by Fogerty v. Fantasy, Inc.*, 510 U.S. 517 (1994). "Impertinent matter consists of statements that do not pertain, and are not necessary, to the issues in question." *Id.* (internal quotations and citations omitted). Motions to strike are regarded with disfavor because they are often used as delaying tactics and because of the limited importance of pleadings in federal practice. *Cal. Dep't of Toxic Substance Control*, 217 F. Supp. 2d at 1033.

Courts within this District and within the Ninth Circuit have determined that "motions to strike are not the proper vehicle for seeking dismissal of class allegations." *Tasion Commc'ns, Inc. v. Ubiquiti Networks, Inc.*, No. 13-cv-01803-EMC, 2014 WL 1048710, at *3 (N.D. Cal. Mar. 14, 2014); *see also, e.g.*, *DeLux Cab, LLC v. Uber Techs., Inc.*, No. 16-cv-3057-CAB-JMA, 2017 WL 1354791, at *8 (S.D. Cal. Apr. 13, 2017); *Astiana v. Ben & Jerry's Homemade, Inc.*, No. 10-cv-04387-PJH, 2011 WL 2111796, at *15 (N.D. Cal. May 26, 2011). To the extent Walmart relies on Rule 12(f), the Court concludes the class allegations are not redundant, immaterial, impertinent, or scandalous. *See, e.g.*, *Beal v. Lifetouch, Inc.*, No. 10-cv-08454 JST (MLGx), 2011 WL 995884, at *7 (C.D. Cal. March 15, 2011).

Walmart also argues that the Court should strike the allegations pursuant to Rule 23, which provides that a court may "require that the pleadings be amended to eliminate allegations about representation of absent persons and that the action proceed accordingly." Fed. R. Civ. P. 23(d)(1)(D); *see also* Fed. R. Civ. P. 23(c)(1)(A) (a court may determine whether to certify the action as a class action at "an early practicable time"). Even under this rule, courts have determined that "class allegations are not tested at the pleading stage and are instead scrutinized after a party has filed a motion for class certification." *Yastrab v. Apple Inc.*, No. 14-cv-01974-EJD, 2015 WL 1307163, at *8 (N.D. Cal. Mar. 23, 2015); *cf. In re Wal-Mart Stores, Inc. Wage & Hour Litig.*, 505 F. Supp. 2d 609, 616 (N.D. Cal. 2007) ("[T]he granting of motions to dismiss class allegations before discovery has commenced is rare."). However, in some cases the issue may be "plain enough" based on the pleadings. *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 160 (1982); *see also Tietsworth v. Sears*, 720 F. Supp. 2d 1123, 1146 (N.D. Cal. 2010) (under Rule 23(d), a court "has authority to strike class allegations prior to discovery if the complaint demonstrates that a class action cannot be maintained").

***11** Walmart asserts that Plaintiff did not assent to the version of the TOU containing the arbitration agreement, which makes him atypical and inadequate to represent the putative class members who are subject to the arbitration agreement. Walmart bases this argument on an assertion Plaintiff made in a declaration attached to his opposition to Walmart's withdrawn motion to compel arbitration.[4] But "[t]he effect of withdrawal of a motion is to leave the record

as it stood prior to the filing as though the motion had never been made." *Davis v. United States*, No. 5:07-cv-00481-VAP-OP, 2010 WL 334502, at *2 (C.D. Cal. Jan. 28, 2010); *see also Larson v. Harman-Mgmt. Corp.*, No. 1:16-cv-00219-DAD-SKO, 2018 WL 3326695, at *1 (E.D. Cal. Mar. 22, 2018) ("Withdrawal of a motion has a practical effect as if the party had never brought the motion.").

Here, the complaint lacks allegations establishing whether or not Plaintiff consented to arbitration, and Walmart offers no other evidence of Plaintiff's alleged opt-out and no argument as to why the Court should consider evidence that was submitted in opposition to a withdrawn motion. Indeed, in withdrawing its motion to compel, Walmart confirmed the need for additional discovery to resolve issues related to arbitration. The fact that many issues surrounding arbitration remain in dispute sets this case apart from those cited by Walmart, in which the defendants had clearly established that the plaintiffs were not subject to the respective arbitration agreements. While the arbitration issue may prove to be a strong argument against class certification, the Court cannot conclude based on the pleadings that a class action cannot be maintained. Accordingly, the Court DENIES Walmart's motion to strike the class allegations.

CONCLUSION

For the foregoing reasons, the Court GRANTS Walmart's motion to dismiss and DENIES Walmart's motion to strike the class allegations. The Court GRANTS Plaintiff leave to amend to cure the deficiencies identified in this Order, if he can do so consistent with his obligations under Federal Rule of Civil Procedure 11. Plaintiff shall file and serve his amended complaint within 21 days.

Furthermore, the Court admonishes Plaintiff to review and comply with the Court's Local Rules and this Court's Standing Orders. Plaintiff's opposition to the motion to dismiss and the opposition to the motion to strike exceeded this Court's page limitations. *See* Civil Standing Orders ¶ 7. Future non-compliant filings will be stricken.

IT IS SO ORDERED.

All Citations

Slip Copy, 2021 WL 2520103

Footnotes

1 Plaintiff argues in opposition that he did not cancel his credit cards, and "does not even know for sure which credit cards were compromised, as he does not know which were used." (Opp. at 16.) This argument, however, if true, undermines any argument that Plaintiff has suffered injury.

2 Walmart asks the Court to take judicial notice of several iterations of Walmart.com's Terms of Use, the effective dates of which span the alleged class period, pursuant to Rule 201 of the Federal Rules of Evidence. (*See* Dkt. No. 34, Request for Judicial Notice ("RJN").) Plaintiff does not oppose Walmart's request. Courts have routinely taken judicial notice of contents of web pages available through the Wayback Machine as facts that can be accurately and readily determined from sources whose accuracy cannot be questioned. *See* *United States ex rel. Hong v. Newport Sensors, Inc.*, No. SA 13-CV-1164-JLS (JPRX), 2016 WL 8929246, at *3 (C.D. Cal. May 19, 2016). Accordingly, the Court GRANTS Walmart's request and takes judicial notice of the versions of the Terms of Use attached as Exhibits A-I.

3 Plaintiff does not allege when he created his Walmart account so it unclear to which version of the TOU he assented. However, each version appears contains a limitation of liability provision that would apply to the contract claims.

4 Civil Local Rule 7-7(e) permits a moving party to withdraw its motion within seven days after an opposition is filed. The filing of a timely notice of withdrawal is self-executing. *See* L.R. 7-7(e); *see also Thomas v. Evans*,

No. C 06-3581 MMC (PR), 2008 WL 2024954, at *1 (N.D. Cal. May 9, 2008). Walmart filed a motion to compel arbitration on October 9, 2020. Plaintiff filed his opposition to Walmart's motion to compel arbitration on October 23, 2020. Walmart timely filed its notice of withdrawal on October 29, 2020.

End of Document

EXHIBIT 7

501 F.Supp.3d 898
United States District Court, S.D. California.

Vicki STASI, Shane White, and Crystal Garcia, individually and on behalf of all others similarly situated, Plaintiffs,
v.
INMEDIATA HEALTH GROUP CORP., Defendant.

Case No.: 19cv2353 JM (LL)
|
Signed 11/19/2020

Synopsis

Background: Patients whose personal and medical information was compromised as a result of medical billing provider's data breach filed putative class action against billing provider, alleging claims for negligence, breach of contract, unjust enrichment, invasion of privacy, and violations of California Confidentiality of Medical Information Act (CMIA), California Consumer Privacy Act, California Consumer Records Act, Minnesota Health Records Act, and California Constitution. Defendant moved to dismiss for lack of subject matter jurisdiction and for failure to state a claim.

Holdings: The District Court, Jeffrey T. Miller, Senior District Judge, held that:

[1] patients sufficiently alleged a concrete statutory privacy injury under CMIA to confer Article III standing;

[2] economic loss doctrine did not apply;

[3] patients sufficiently alleged a common law duty under California law, as element of negligence claim;

[4] patients sufficiently alleged breach of duty, as element of negligence claim;

[5] patients alleged plausible damages, as element of negligence claim;

[6] allegations that contracts existed and contained terms protecting confidential medical information were sufficient to allege a breach of contract claim based on third party beneficiary theory; and

[7] patients sufficiently alleged damages, as element of breach of contract claim.

Motions granted in part and denied in part.

Procedural Posture(s): Motion to Dismiss for Lack of Subject Matter Jurisdiction; Motion to Dismiss for Failure to State a Claim.

West Headnotes (49)

[1] Federal Courts Dismissal or other disposition

Dismissal for lack of subject matter jurisdiction is appropriate if the complaint, considered in its entirety, on its face fails to allege facts sufficient to establish subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1).

[2] Federal Courts Presumptions and burden of proof

The plaintiff bears the burden of establishing subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1).

[3] Federal Courts Pleadings and motions

In a facial attack on the pleadings on a motion to dismiss for lack of subject matter jurisdiction, the court accepts the allegations in the complaint as true and draws all reasonable inferences in the plaintiff's favor. Fed. R. Civ. P. 12(b)(1).

[4] **Federal Civil Procedure** Construction of pleadings

In deciding a motion to dismiss for failure to state a claim, the allegations must be construed in the light most favorable to plaintiff. Fed. R. Civ. P. 12(b)(6).

[5] **Federal Civil Procedure** Matters deemed admitted; acceptance as true of allegations in complaint

While a court must take all factual allegations in the complaint as true when deciding a motion to dismiss for failure to state a claim, it is not bound to accept as true a legal conclusion couched as a factual allegation. Fed. R. Civ. P. 12(b)(6).

[6] **Federal Civil Procedure** Matters considered in general

Although the court generally cannot consider facts outside the complaint in ruling on a motion to dismiss for failure to state a claim, it may consider documents that are referenced in the complaint. Fed. R. Civ. P. 12(b)(6).

[7] **Federal Civil Procedure** In general; injury or interest

Federal Courts Case or Controversy Requirement

A suit brought by a plaintiff without Article III standing is not a case or controversy, and an Article III federal court therefore lacks subject matter jurisdiction over the suit. U.S. Const. Art. 3, § 2, cl.1; Fed. R. Civ. P. 12(b)(1).

[8] **Federal Civil Procedure** In general; injury or interest

Federal Civil Procedure Causation; redressability

Standing requires the plaintiff to have suffered an injury in fact that is fairly traceable to the challenged conduct of the defendant, and is likely to be redressed by a favorable judicial decision.

[9] **Federal Civil Procedure** In general; injury or interest

An injury in fact, required for standing, is an invasion of a legally protected interest which is concrete and particularized, actual or imminent, and not conjectural or hypothetical.

[10] **Federal Civil Procedure** In general; injury or interest

The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing the elements of Article III jurisdiction. U.S. Const. Art. 3, § 2, cl.1.

[11] **Federal Civil Procedure** Pleading

At the motion to dismiss stage, standing is demonstrated through allegations of specific facts plausibly explaining that standing requirements are met.

[12] **Federal Civil Procedure** Construction of pleadings

Federal Civil Procedure Matters deemed admitted; acceptance as true of allegations in complaint

In determining whether a plaintiff has standing at the motion to dismiss stage, the court is to accept as true all material allegations of the complaint, and construe the complaint in favor of the complaining party.

[13] **Federal Civil Procedure** Pleading

General factual allegations of injury resulting from the defendant's conduct may suffice to establish standing, and the court presumes that

general allegations embrace those specific facts that are necessary to support the claim.

[14] **Federal Civil Procedure** In general; injury or interest

The question of standing is distinct from the merits of the plaintiff's claim.

[15] **Federal Civil Procedure** In general; injury or interest

Intangible injuries based on violation of a statute can be concrete so as to establish an injury in fact required for standing.

[16] **Federal Civil Procedure** In general; injury or interest

General principles that are instructive for assessing whether an intangible injury is concrete so as to establish an injury in fact required for standing include (1) whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts, and (2) whether, in Congress' judgment, the intangible harm meets minimum Article III requirements even though it previously did not. U.S. Const. Art. 3, § 2, cl.1.

[17] **Federal Civil Procedure** In general; injury or interest

A plaintiff cannot allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III, but the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact required for standing. U.S. Const. Art. 3, § 2, cl.1.

[18] **Health** Confidentiality; patient records

Patients sufficiently alleged a concrete statutory privacy injury under California Confidentiality of Medical Information Act (CMIA) to confer Article III standing to bring claims against medical billing provider in connection with intangible injury resulting from medical billing provider allowing disclosure of patients' personal and medical information on internet due to data breach, by alleging they suffered a privacy injury by having sensitive medical information disclosed and available for copying, spent time and money addressing issues from data breach, and noticed an increase in spam e-mails, calls, or both, from persons apparently attempting to defraud them; alleged harm was closely related to one traditionally protected at law, and which CMIA was intended to prevent. U.S. Const. Art. 3, § 2, cl.1; Cal. Civ. Code § 56.36(b).

[19] **Federal Civil Procedure** In general; injury or interest

The court has an independent obligation to assure plaintiffs' Article III standing. U.S. Const. Art. 3, § 2, cl.1.

[20] **Records** Persons entitled to pursue proceedings; standing

Every violation of a substantive provision of a privacy-related statute, and every disclosure of information protected by that provision, presents the precise harm and infringes the same privacy interests Congress sought to protect, which gives rise to a concrete injury sufficient to confer standing.

[21] **Federal Civil Procedure** Claim for relief in general

A plaintiff may suffer Article III injury and yet fail to plead a proper cause of action. U.S. Const. Art. 3, § 2, cl.1.

[22] **Negligence** Elements in general

The elements of a negligence claim under California law are duty, breach, causation, and injury.

[23] **Torts** Economic loss doctrine

Under the economic loss doctrine, purely economic losses are not recoverable in tort under California law.

1 Cases that cite this headnote

[24] **Negligence** Economic loss doctrine

In the absence of personal injury, physical damage to property, a special relationship between the parties, or some other common law exception to the rule, recovery of purely economic loss for negligence is foreclosed under California law.

1 Cases that cite this headnote

[25] **Health** Confidentiality; patient records

Economic loss doctrine did not apply to preclude patients' negligence claim under California law against medical billing provider concerning data breach with respect to patients' compromised personal and medical information, where patients alleged they suffered a privacy injury by having their sensitive medical information disclosed, noticed an increase in spam or phishing e-mails and/or calls, and expended time responding to data breach, and that parties were not in privity of contract, there was no commercial activity between parties that went awry, and case did not involve a defective product or services resulting in mere disappointed expectations.

[26] **Health** Confidentiality; patient records

Statutory protection afforded to medical information was rooted in common law duties traditionally serving as the basis for lawsuits, including duty not to publicly disclose private facts, and therefore, to the extent the economic loss rule applied to patients' negligence claim against medical billing providers with respect to data breach which compromised patients' personal and medical information, it was plausible a common law exception to rule also applied, such that negligence claim under California law was not defeated by economic loss doctrine.

1 Cases that cite this headnote

[27] **Health** Confidentiality; patient records

Patients sufficiently alleged a common law duty under California law, as element of negligence claim against medical billing provider in connection with data breach with respect to patients' personal and medical information, despite fact that patients were not medical billing provider's customers or otherwise in privity with medical billing provider, by alleging that medical billing provider owed patients a duty to safeguard their personal and medical information as consistent with medical privacy statutes and industry standards; state and federal law already required such protection, and, in the case of state law, already allowed for a private right of action, and burden of duty appeared especially light given provider's position that errant web page setting was culprit of data breach.

[28] **Health** Confidentiality; patient records

Patients sufficiently alleged that medical billing provider breached duty to safeguard patients' personal and medical information, as element of negligence claim under California law in connection with data breach which compromised patients' personal and medical information, by alleging that patients lost time and money responding to provider's data breach notification, that they noticed an increase in spam/phishing e-mails and/or calls, and that provider failed to protect medical information.

1 Cases that cite this headnote

[29] **Health** Confidentiality; patient records

Patients failed to sufficiently allege causation in connection with allegation that one patient actually experienced identity theft from data breach with respect to personal and medical information, but not financial information, thus precluding a plausible negligence claim under California law, where information may have been compromised during a previous, unrelated data breach, and allegations of identity theft involved financial information resulting in fraudulent charges on credit card.

2 Cases that cite this headnote

[30] **Health** Confidentiality; patient records

It was plausible that lost time and increase in spam/phishing which patients allegedly suffered was caused by alleged breach of medical billing provider's duty to protect personal and medical information in connection with data breach resulting in patients' confidential medical information being posted on the internet, as element of negligence claim under California law.

1 Cases that cite this headnote

[31] **Health** Confidentiality; patient records

Patients alleged plausible damages in the form of lost time, as element of negligence claim under California law against medical billing provider in connection with data breach resulting from errant web page setting which compromised patients' personal and medical information, by alleging that time was spent dealing with issues related to data breach and trying to make sure patients had not and would not become further victimized because of data breach, and that patients noticed increase in spam/phishing e-mails or calls or both from persons apparently attempting to defraud patients during time when provider became aware of breach.

[32] **Health** Confidentiality; patient records

Patients sufficiently alleged that one patient suffered damages in the form of lost money, as element of negligence claim under California law in connection with data breach caused by errant web page setting which resulted in posting patients' personal and medical information on the internet, by alleging that patient spent her own money addressing issues arising from data breach, although patients did not specify what money was spent on or what issues were addressed; in deciding motion to dismiss for failure to state a claim it was reasonable to infer that patient's out-of-pocket expenses involved some form of identity theft protection. Fed. R. Civ. P. 12(b)(6).

[33] **Health** Confidentiality; patient records

Negligence per se doctrine supported plausibility of patients' negligence claim under California law against medical billing provider in connection with data breach that resulted in posting on internet patients' confidential medical information, which was protected by California Confidentiality of Medical Information Act (CMIA); in deciding motion to dismiss for failure to state a claim, it was reasonable to infer that alleged injuries resulting from posting of medical information on the internet were the injuries the statute was intended to prevent, and that patients, as persons who initially provided confidential medical information that provider possessed, were within class of persons for whose protection the statute was adopted. Cal. Civ. Code § 56.36(b)(1); Fed. R. Civ. P. 12(b)(6).

[34] **Negligence** Duty based upon statute or other regulation

The negligence per se doctrine does not obviate the need for plaintiffs to show a viable and independent duty.

[35] **Contracts** Agreement for Benefit of Third Person

The standard to achieve third party beneficiary status is a high one in a breach of contract case under California law.

[36] **Health** Confidentiality; patient records

Patients' allegations that contracts with medical billing provider existed and contained terms protecting patients' confidential medical information were sufficient to allege a breach of contract claim under California law based on third party beneficiary theory in connection with data breach resulting in patients' confidential medical information being posted on internet, although patients did not provide specific contract terms; allegations were sufficiently factual to give fair notice and to enable medical billing provider to defend itself effectively, and without discovery, it was not clear what more patients could plead, or what more medical billing provider would need to be able to defend against patients' claims that they were third party beneficiaries of medical billing provider's contracts.

[37] **Federal Civil Procedure** Information and belief

Federal Courts Pleadings and motions

In the early stages of litigation, plaintiffs may base their allegations, even jurisdictional ones, on information and belief when the allegations include facts that are primarily within the defendant's knowledge.

[38] **Health** Confidentiality; patient records

Patients sufficiently alleged damages, as element of breach of contract claim under California law against medical billing provider that posted patients' confidential medical information on internet due to data breach caused by errant web page setting, by alleging that one patient spent her own money addressing issues arising from data breach, which was sufficient to infer that she spent money on some form of identity theft protection.

1 Cases that cite this headnote

[39] **Implied and Constructive Contracts** Unjust enrichment

To the extent that patients actually and sufficiently alleged unjust enrichment under Florida and Minnesota law against medical billing provider in connection with posting of patients' confidential medical information on the internet due to data breach caused by errant web page setting, those claims survived medical billing provider's motion to dismiss for failure to state a claim, even though patients did not list their purported claims for unjust enrichment under Florida or Minnesota law as separate claims, and only made passing reference to Florida and Minnesota law, since medical billing provider did not challenge unjust enrichment claims under Florida or Minnesota law. Fed. R. Civ. P. 12(b)(6).

[40] **Health** Confidentiality; patient records

Under California law, in order to plead a violation of section of California Confidentiality of Medical Information Act (CMIA) which mandates that health care providers and contractors shall not disclose medical information the plaintiff must plead an affirmative communicative act by the defendant, which does not occur if the information is stolen.

Cal. Civ. Code § 56.10(a).

[41] **Health** Confidentiality; patient records

Patients failed to allege that medical billing provider intentionally posted patients' medical information on internet, or that whatever affirmative act might have caused their information to become accessible via the internet was done with the intent to communicate that information, and thus patients failed to state a claim for violation of section of California Confidentiality of Medical Information Act (CMIA) which mandates that health care providers and contractors shall not disclose medical information, even though it was reasonable to infer that some affirmative act by provider caused errant web page setting that allegedly caused data breach and made patients' information accessible via the internet. Cal. Civ. Code § 56.10(a).

[42] **Health** Confidentiality; patient records

To sufficiently plead actual or nominal damages under California Confidentiality of Medical Information Act (CMIA), it is insufficient for the plaintiff to plead that the defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information; rather, the plaintiff must also plead that information was negligently released. Cal. Civ. Code § 56.36(b).

[43] **Health** Confidentiality; patient records

Patients alleged a plausible claim against medical billing provider based on violations of sections of California Confidentiality of Medical Information Act (CMIA) establishing a duty to preserve confidentiality and allowing a private right of action for negligent release, by alleging that provider posted patients' medical information on internet due to data breach purportedly caused by errant web page setting, making it searchable, findable, viewable, printable, copyable, and downloadable by anyone in the world with an internet connection, and that patients believed their information was viewed by unauthorized persons. Cal. Civ. Code §§ 56.36(b), 56.101(a).

1 Cases that cite this headnote

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

Health Confidentiality; patient records

Patients alleged a plausible claim against medical billing provider based on violation of California Consumer Privacy Act (CCPA), which provides a private right of action for actual or statutory damages to any consumer whose nonencrypted and nonredacted personal information 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, by alleging that their non-medical information was posted on the internet as a result of data breach, and that their information was viewed by unauthorized persons. Cal. Civ. Code § 1798.150(a).

3 Cases that cite this headnote

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

Health Confidentiality; patient records

Patients alleged a plausible claim against medical billing provider based on violations of the California Consumer Records Act (CCRA), requiring disclosure of a data breach in the most expedient time possible and without unreasonable delay, by alleging that by taking 81 days to inform patients of data breach, medical billing provider acted with unreasonable delay, and that because of the delay patients were prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze which could have prevented some of their damages because their information would have

been less valuable to identity thieves. Cal. Civ. Code § 1798.82(a).

[46] **Health** Confidentiality; patient records

Patients alleged a plausible claim against medical billing provider based on violations of Minnesota Health Records Act (MHRA), by alleging that medical billing provider released their health records without first obtaining consent or authorization, and negligently or intentionally released patients' health records by posting information on the internet for an unknown period of time, and that patients' information was viewed by unauthorized persons. Minn. Stat. Ann. §§ 144.29-144.34.

[47] **Constitutional Law** Right to Privacy

Constitutional Law Reasonable, justifiable, or legitimate expectation

To support a privacy claim under the California Constitution, plaintiffs must show: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy. Cal. Const. art. 1, § 1.

1 Cases that cite this headnote

[48] **Health** Confidentiality; patient records

Plaintiffs have a legally protected privacy interest in their medical information.

1 Cases that cite this headnote

[49] **Constitutional Law** Medical records or information

Health Confidentiality; patient records

Patients alleged a plausible violation of the California Constitution's privacy provision in connection with medical billing provider's posting of patients' medical information on the internet due to data breach; it was reasonable to infer that patients reasonably expected medical billing provider would not post patients' medical information on the internet, negligently or otherwise, and that doing so was a serious invasion of privacy. Cal. Const. art. 1, § 1.

Attorneys and Law Firms

***905** Andrew W. Ferich, Pro Hac Vice, Benjamin F. Johns, Pro Hac Vice, Chimicles Schwartz Kriner & Donaldson-Smith LLP, Haverford, PA, Cornelius Pellman Dukelow, Pro Hac Vice, Abington Cole + Ellery, Tulsa, OK, Tina Wolfson, Bradley K. King, Ahdoot & Wolfson, PC, Burbank, CA, for Plaintiffs.

Jon Peter Kardassakis, Lewis Brisbois Bisgaard & Smith LLP, Los Angeles, CA, for Defendant.

ORDER ON DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT

JEFFREY T. MILLER, United States District Judge

Defendant Inmediata Health Group Corp. ("Inmediata") moves under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) to dismiss the First Amended Complaint ("FAC") of Plaintiffs Vicki Stasi, Shane White, and Crystal Garcia. (Doc. No. 17-1.) The motion has been briefed and the court finds it suitable for submission without oral argument in accordance with Civil Local Rule 7.1(d)(1). For the below reasons, Inmediata's motion to dismiss under Rule 12(b)(1) is **DENIED**, and Inmediata's motion to dismiss under Rule 12(b)(6) is **DENIED IN PART** and **GRANTED IN PART**.

I. BACKGROUND

According to Plaintiffs' FAC, [1] Inmediata provides billing and health record software and service solutions to healthcare providers. (FAC ¶¶ 17, 19.) In January of 2019, Inmediata first learned it was experiencing a "large data breach" resulting in the "unauthorized acquisition, access, use, or disclosure of unsecured protected health information and personal information" of 1,565,338 individuals. (¶ 2.) [2] Plaintiffs' information was "posted on the Internet" and "searchable

and findable by anyone with access to an internet search engine such as Google[.]" (¶ 7.) Plaintiffs' information was "disclosed and released to the entire world – it was viewable online by anyone in the world, printable by anyone in the world, copiable by anyone in the world, and downloadable by anyone in the world." (¶ 8.) The breach did not involve ***906** data thieves or hackers. (¶ 9.) Rather, the exposure was "[d]ue to a webpage setting that permitted search engines to index webpages Inmediata uses for business operations[.]" (¶ 7.)

By letter dated April 22, 2019, Inmediata notified Plaintiffs of a "data security incident that may have resulted in the potential disclosure of [their] personal and medical information." (¶ 24; *see also* Doc. Nos. 16-3, 16-4, 16-5.) Inmediata also filed sample "notice of data security incident" letters with various state attorneys general that mirrored the language of the letters sent to Plaintiffs. (¶ 26.) There were two versions of the letter – one for persons whose social security numbers were part of the breach, and another version for persons whose social security numbers were not part of the breach. (¶ 26 n.1.) Plaintiffs received the version for persons whose social security numbers were *not* part of the breach. (*Id.*) The letters stated that "[i]n January 2019, Inmediata became aware that some of its member patients' electronic patient health information was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website [Inmediata] use[s] for .... business operations." (¶ 27.) The letters also stated that "information potentially impacted by this incident may have included your name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician." (¶ 29.) Inmediata did not offer Plaintiffs fraud insurance or identity monitoring services. (¶ 34.)

On December 9, 2019, Plaintiffs filed a putative class action. On May 5, 2020, Plaintiffs' initial Complaint was dismissed under Rule 12(b)(1). (Doc. No. 15.) On May 19, 2020, Plaintiffs filed their FAC, which included claims for: (1) negligence; (2) breach of contract; (3) unjust enrichment; (4) violation of the California Confidentiality of Medical Information Act; (5) violation of the California Consumer Privacy Act; (6) violation of the California Consumer Records Act; (7) violation of the Minnesota Health Records Act; and (8) invasion of privacy and violation of the California Constitution. (¶¶ 212-324.) Plaintiffs seek to certify a nationwide class consisting of "[a]ll persons .... whose [p]ersonal and [m]edical [i]nformation was compromised as a result of the [d]ata [b]reach announced by Inmediata on or around April 24, 2019." (¶ 199.) Plaintiffs alternatively seek to certify statewide classes for California, Minnesota, and Florida. (¶ 200.)

II. LEGAL STANDARDS

A. Rule 12(b)(1)

[1] **[2]** **[3]** Rule 12(b)(1) allows a party to move for dismissal of an action based on lack of subject matter jurisdiction. "Dismissal for lack of subject matter jurisdiction is appropriate if the complaint, considered in its entirety, on its face fails to allege facts sufficient to establish subject matter jurisdiction." *In re Dynamic Random Access Memory Antitrust Litig.*, 546 F.3d 981, 984-85 (9th Cir. 2008) (citation omitted). The plaintiff bears the burden of establishing subject matter jurisdiction. *United States v. Orr Water Ditch Co.*, 600 F.3d 1152, 1157 (9th Cir. 2010). If the court finds it lacks subject matter jurisdiction at any time, it must dismiss the action. Fed. R. Civ. P. 12(h)(3). In a facial attack on the pleadings under Rule 12(b)(1), the court accepts the allegations in the complaint as true and draws all reasonable inferences in the plaintiff's favor. *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004).

B. Rule 12(b)(6)

[4] **[5]** **[6]** To survive a motion to dismiss under Rule 12(b)(6), the complaint must ***907** contain sufficient facts to state a claim for relief that is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678, 129 S.Ct. 1937. The allegations must be construed in the light most favorable to plaintiff. *Schueneman v. Arena Pharm., Inc.*, 840 F.3d 698, 704 (9th Cir. 2016). While a court must take all factual allegations in the complaint as true, it is "not bound to accept as true a legal conclusion couched as a factual allegation."

Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. In resolving the motion, the court does not weigh evidence, evaluate witness credibility, or consider the likelihood that a plaintiff will prevail at trial. *Twombly*, 550 U.S. at 556, 127 S.Ct. 1955 ("[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of the facts alleged is improbable, and 'that a recovery is very remote and unlikely[.]' "). Although the court generally cannot consider facts outside the complaint in ruling on a Rule 12(b)(6) motion to dismiss, *Arpin v. Santa Clara Valley Transp. Agency*, 261 F.3d 912, 925 (9th Cir. 2001), it may consider documents that are referenced in the complaint, *No. 84 Employer-Teamster Joint Council Pension Trust Fund v. Am. W. Holding Corp.*, 320 F.3d 920, 925 n.2 (9th Cir. 2003).

III. DISCUSSION

A. Standing

[7] **[8]** **[9]** "A suit brought by a plaintiff without Article III standing is not a 'case or controversy,' and an Article III federal court therefore lacks subject matter jurisdiction over the suit." *Cetacean Cmty. v. Bush*, 386 F.3d 1169, 1174 (9th Cir. 2004) (citation omitted). Standing requires the plaintiff to have suffered an injury in fact that is fairly traceable to the challenged conduct of the defendant, and is likely to be redressed by a favorable judicial decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992). An injury in fact is an invasion of a legally protected interest which is concrete and particularized, actual or imminent, and not conjectural or hypothetical. *Id.* at 560, 112 S.Ct. 2130.

[10] **[11]** **[12]** **[13]** **[14]** The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing the elements of Article III jurisdiction. *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231, 110 S.Ct. 596, 107 L.Ed.2d 603 (1990). At the motion to dismiss stage, standing is demonstrated through allegations of specific facts plausibly explaining that standing requirements are met. *Barnum Timber Co. v. Envtl. Prot. Agency*, 633 F.3d 894, 899 (9th Cir. 2011); *see also Warth v. Seldin*, 422 U.S. 490, 518, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975) ("It is the responsibility of the complainant clearly to allege facts demonstrating that he is a proper party to invoke judicial resolution of the dispute and the exercise of the court's remedial powers."). However, "the court is to 'accept as true all material allegations of the complaint, and .... construe the complaint in favor of the complaining party.' " *Levine v. Vilsack*, 587 F.3d 986, 991 (9th Cir. 2009) (quoting *Thomas v. Mundell*, 572 F.3d 756, 760 (9th Cir. 2009)). "[G]eneral factual allegations of injury resulting from the defendant's conduct may suffice," and the court "presume[s] that general allegations embrace those specific facts that are necessary to support the claim." *Lujan*, 504 U.S. at 561, 112 S.Ct. 2130 (quotation and alteration omitted). The question of standing is ***908** "distinct from the merits" of the plaintiff's claim. *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011); *see also Warth*, 422 U.S. at 500, 95 S.Ct. 2197 ("[S]tanding in no way depends on the merits of the plaintiff's contention that particular conduct is illegal[.]").

1. Statutory Standing

[15] **[16]** **[17]** Intangible injuries based on violation of a statute can be concrete. *Spokeo, Inc. v. Robins*, —— U.S. ——, 136 S. Ct. 1540, 1549, 194 L.Ed.2d 635 (2016). "[G]eneral principles" that are "instructive" for assessing whether an intangible injury is concrete include (1) "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," and (2) whether, in Congress' judgment, the intangible harm meets minimum Article III requirements even though it previously did not. *Id.* at 1549. A plaintiff cannot allege "a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III," but "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact." *Id.*

[18] **[19]** Plaintiffs argue they sufficiently pled concrete injury by pleading that Inmediata violated the California Confidentiality of Medical Information Act ("CMIA"), CAL. CIV. CODE §§ 56-56.265. (Doc. No. 22 at 10-12.) In support of this argument, Plaintiffs state that CMIA was "enacted to protect people such as Plaintiffs from precisely this sort of long-recognized violation of privacy rights in [confidential medical information]." (*Id.* at 10.) Plaintiffs also state that CMIA was "established to protect concrete privacy interests in medical privacy that go far beyond bare procedural requirements, and [Inmediata's] violations of [CMIA] directly implicate Plaintiffs' interests in those same, concrete, medical privacy rights," (*id.*), and that the California legislature declared the right to privacy "fundamental," (*id.* at 11, 12).[3] As discussed in greater detail below, CMIA prohibits the unauthorized "disclosure" of medical information, the negligent maintenance of medical information, and the negligent "release" of medical information.[4] CAL. CIV. CODE §§ 56.10(a), 56.101(a), 56.36(b). The statute also provides for nominal damages without having to show the plaintiff "suffered or was threatened with actual damages." *Id.* § 56.36(b)(1). Plaintiffs allege that by "posting"[5] their private medical information on the internet, Inmediata violated CMIA by disclosing the information, negligently failing to preserve its confidentiality, and negligently releasing the information. (¶¶ 269-71.)

a. Ninth Circuit Precedent

At the outset, the alleged intangible injury resulting from "posting" or allowing access to disclosure of Plaintiffs' medical ***909** information on the internet in violation of CMIA is, at first blush, just as concrete as the intangible injuries the Ninth Circuit has found to be concrete based on violations of other privacy-related statutes. *See* *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1112 (9th Cir. 2020) (alleging Facebook scanned plaintiffs' private messages looking for links to web pages, then allowed third parties to show that the link counted as a "like" on their websites, in violation of the Electronic Communications Privacy Act (ECPA) and the California Invasion of Privacy Act (CIPA)); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020) ("*Facebook Tracking*") (alleging Facebook tracked users' browsing histories when they visited third-party websites, then compiled their browsing histories into profiles which were sold to advertisers in violation of federal and state statutes, including the CIPA); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019) (alleging Facebook subjected the plaintiffs to facial recognition technology in violation of state biometric privacy statute), *cert. denied*, —— U.S. ——, 140 S. Ct. 937, 205 L.Ed.2d 524 (2020); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017) (alleging ESPN shared plaintiff's personally identifiable information with a third party in violation of the Video Privacy Protection Act (VPPA)); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (alleging plaintiff received two unsolicited text messages advertising a gym membership in violation of the Telephone Consumer Protection Act (TCPA)); *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1117 (9th Cir. 2017) ("*Spokeo II*") (alleging credit reporting agency published incorrect biographical information about the plaintiff on the internet in violation of procedural requirements of the Fair Credit Reporting Act (FCRA)). For example, it cannot reasonably be argued that the unwanted receipt of text messages advertising a gym membership, annoying as they may be, is a more serious violation of a statutorily protected privacy right than having one's medical information accessible via the internet for an unknown period of time. Medical information is also just as private and sensitive as the links included in messages sent via Facebook, facial biometric information, and a person's video watching history. *See* *Campbell*, 951 F.3d at 1112; *Patel*, 932 F.3d at 1274; *Eichenberger*, 876 F.3d at 981. As stated in *Campbell*, "[t]here is no meaningful distinction between the concrete, substantive privacy interests protected by the statutes at issue in *Patel*, *Eichenberger*, and *Van Patten* and the interests protected by the provisions of [the privacy statute] at issue in this case." 951 F.3d at 1118.

Although the Ninth Circuit has found, in near uniformity, that intangible injuries based on alleged violations of privacy-related statutes are sufficiently concrete, Inmediata nonetheless urges the court to follow *Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776 (9th Cir. 2018). In

Bassett, the court held the plaintiff did not sufficiently plead a concrete injury by alleging that a parking garage displayed his unredacted credit card expiration date on his receipt, in alleged violation of the FCRA, where the information was not seen by anyone else. *Id.* at 783. The court reasoned, "[w]e need not answer whether a tree falling in the forest makes a sound when no one is there to hear it." *Id.* *Bassett* is distinguishable, however, because in *Bassett* it was known that nobody else saw, or could have seen, the plaintiffs' protected information. Here, Plaintiffs repeatedly allege their information "was viewed by unauthorized persons." (¶¶ 269-271, 277.) Although the basis for Plaintiffs' assertion that their information was actually viewed is sketchy (and, absent ultimate proof, would likely be fatal for Plaintiffs' case in this regard), it is reasonable to infer the information could have been viewed or ***910** copied once available on the internet. (*See* ¶¶ 7-8.) In other words, unlike in *Bassett*, the tree falling in the woods question is unavoidable here. Accordingly, even prior to applying the *Spokeo* test, Ninth Circuit precedent strongly supported the concreteness of Plaintiffs' alleged injury resulting from a violation of CMIA.

b. Traditional Harm

Additionally, the harm that results from "posting" medical information on the internet has a close relationship to harm that has traditionally been regarded as providing a basis for a lawsuit, especially the public disclosure of private facts. *See* *Forsher v. Bugliosi*, 26 Cal. 3d 792, 808, 163 Cal.Rptr. 628, 608 P.2d 716 (1980) (recognizing public disclosure of private facts as a type of invasion of privacy claim); *see also* *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763, 109 S.Ct. 1468, 103 L.Ed.2d 774 (1989) ("[B]oth the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."). The Ninth Circuit consistently recognizes that actions based on statutory privacy rights resemble privacy-related claims long available at common law. *See* *Campbell*, 951 F.3d at 1118 ("The reasons articulated by the legislatures that enacted ECPA and CIPA further indicate that the provisions at issue in this case reflect statutory modernizations of the privacy protections available at common law."); *Patel*, 932 F.3d at 1271-72 (supporting standing based on state biometric data statute because "[p]rivacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts' "); *Eichenberger*, 876 F.3d at 981 (VPPA violations resemble violations of the right to privacy that have "long been actionable at common law," including invasion of privacy, and noting that "privacy torts, such as intrusion of seclusion, do not always require additional consequences to be actionable"); *Van Patten*, 847 F.3d at 1043 (TCPA actions resemble "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts, and the right of privacy is recognized by most states"); *Spokeo II*, 867 F.3d at 1114 (FCRA rights resemble the right to prevent the dissemination of private information and right to bring lawsuits based on the unauthorized disclosure of a person's private information). Accordingly, Plaintiffs' alleged harm is closely related to one traditionally protected at law.

c. Legislative Judgment

Finally, it is reasonable to infer that "posting" Plaintiffs' medical information on the internet constitutes a breach of confidentiality that is precisely the type of harm CMIA was intended to prevent as CMIA expressly provides that actionable injury results from the negligent "release" of medical information regardless of whether the plaintiff "suffered or was threatened with actual damages." *See* CAL. CIV. CODE § 56.36(b). The Ninth Circuit has repeatedly found the express abdication of the requirement for actual damages in privacy-related statutes supports standing based on violations of those statutes. *See* *Patel*, 932 F.3d at 1269; *Eichenberger*, 876 F.3d at 981; *Van Patten*, 847 F.3d at 1043. [6]

***911** Although neither party discusses the legislative history of CMIA, the plain language of the statute demonstrates that, in the California legislature's judgment, [7] the provisions of CMIA at issue here are substantive, not procedural. *See also* 1999 Cal. Legis. Serv. Ch. 526 (S.B. 19) ("The bill

would .... create a right of action to recover damages, as specified, for any individual whose confidential information or records are negligently released and would additionally provide for specified administrative and civil penalties."); *Brown v. Mortensen*, 51 Cal. 4th 1052, 1070-71, 126 Cal.Rptr.3d 428, 253 P.3d 522 (2011) ("[CMIA] is intended to protect the confidentiality of individually identifiable medical information obtained from a patient .... [T]he interest protected is an interest in informational privacy[.]") (citation and internal quotation marks omitted); *Heller v. Norcal Mut. Ins. Co.*, 8 Cal. 4th 30, 38, 32 Cal.Rptr.2d 200, 876 P.2d 999 (1994) ("[CMIA] was originally enacted in 1979 to provide for the confidentiality of individually identifiable medical information[.]") (citation and internal quotation marks omitted).

[20] As explained in *Eichenberger*, "every violation" of a substantive provision of a privacy-related statute, and "every disclosure" of information protected by that provision, "presents the precise harm and infringes the same privacy interests Congress sought to protect." 876 F.3d at 984; *see also* *Facebook Tracking*, 956 F.3d at 598 (finding that various privacy-related statutes "codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing"); *Campbell*, 951 F.3d at 1117 ("When .... a statutory provision identifies a substantive right that is infringed any time it is violated, a plaintiff bringing a claim under that provision 'need not allege any further harm to have standing.' ") (citation omitted); *Patel*, 932 F.3d at 1274 (violation of a biometric privacy statute would "necessarily violate the plaintiffs' substantive privacy interests"). At this early stage in the litigation, nothing in the record suggests Plaintiffs must provide additional proof of the concreteness of their injury beyond their allegations of CMIA violations. [8] Accordingly, Plaintiffs have adequately alleged standing. [9]

***912 2. Additional Grounds**

Plaintiffs also allege they suffered "a privacy injury by having their sensitive medical information disclosed, irrespective of whether or not they subsequently suffered identity fraud, or incurred any mitigation damages." (¶ 284.) The concreteness of this injury is supported by *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019), in which the district court found the plaintiffs' allegation that their "sensitive information was disseminated to third parties in violation of their privacy" was sufficient, by itself, to confer standing, even where no theft or hack of the information occurred and the "sensitive information" did not include social security numbers, financial information, or medical information. The district court rejected Facebook's argument that "a 'bare' privacy violation, without 'credible risk of real-world harm' such as identity theft or other economic consequences, cannot rise to the level of an Article III injury." *Id.* at 786-87. To find otherwise, the court reasoned, would "disregard the importance of privacy in our society, not to mention the historic role of the federal judiciary in protecting it" as recognized by "countless federal laws designed to protect our privacy[.]" *Id.* at 786 (citing, inter alia, HIPAA).

Additionally, at least one district court has found an allegation that the plaintiff "received extensive 'phishing' emails and text messages [and] spent as much as an hour managing the aftermath of the data breach" was sufficient to allege injury in fact. *See* *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1035 (N.D. Cal. 2019) ("As consequences of this data breach continue to unfold, so too, will plaintiff's invested time. More phishing e-mails will pile up. At this stage, the time loss alleged suffices."). Here, Plaintiffs allege they spent time "dealing with" and "addressing" issues arising from Inmediata's breach notification. (¶¶ 139, 163, 195.) Plaintiffs also allege they noticed an "increase in spam/phishing" e-mails, calls, or both, from "persons apparently attempting to defraud" them. (¶¶ 136, 157, 192.)

Finally, district courts have found that out-of-pocket expenses are sufficient to confer standing in data breach cases. *See* *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, Case No. 16-MD-02752-LHK, 2017 WL 3727318, at *16 (N.D. Cal. Aug. 30, 2017) (listing cases). Here, Plaintiffs allege that Ms. Garcia spent her own money "addressing issues" arising from the breach. (¶ 195.) Accordingly, these cases serve as additional support for the concreteness of Plaintiffs' alleged injuries. [10]

B. Individual Claims

[21] A plaintiff may suffer Article III injury and yet fail to plead a proper cause of action. *Doe v. Chao*, 540 U.S. 614, 624-25, 124 S.Ct. 1204, 157 L.Ed.2d 1122 (2004). Inmediata argues that Plaintiffs' individual claims for negligence, breach of contract, unjust enrichment, violation of state privacy statutes, and the California Constitution should be dismissed under Rule 12(b)(6). For the below reasons, this argument is mostly unavailing.

1. Negligence

[22] The elements of a negligence claim under California law are duty, breach, causation, and injury. *Vasilenko v. Grace Family Church*, 3 Cal. 5th 1077, 1083, 224 Cal.Rptr.3d 846, 404 P.3d 1196 (2017). Inmediata argues that Plaintiffs' negligence claim is barred by California's economic loss doctrine. (Doc. No. 17-1 at ***913** 19-20.) Inmediata also makes arguments with respect to Plaintiffs' allegations of duty, causation, and damages. (*Id.* at 20-21.)

a. Economic Loss Doctrine

[23] **[24]** Under the economic loss doctrine, "purely economic losses are not recoverable in tort." *NuCal Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) (citation omitted). In the absence of personal injury, physical damage to property, a special relationship between the parties, or some other common law exception to the rule, recovery of purely economic loss for negligence is foreclosed. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 803-04, 157 Cal.Rptr. 407, 598 P.2d 60 (1979). Inmediata argues that Plaintiffs' negligence claim is barred by the economic loss doctrine because Plaintiffs do not allege personal injury or property damage. (Doc. No. 17-1 at 19-20.) In support of this argument, Inmediata cites *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, Case No.: 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016), in which the district court found the economic loss doctrine barred the plaintiffs' negligence claim because they alleged purely economic damages, i.e. "theft of their credit card information, costs associated with prevention of identity theft, and costs associated with time spent and loss of productivity."

[25] *Dugas* is not persuasive, however, because even though Plaintiffs allege they lost time responding to Inmediata's breach notification, (*see* ¶¶ 139, 163, 195), they do not necessarily base their allegations on the "costs" of their lost time and lost productivity. Moreover, unlike in *Dugas*, the compromised information here includes medical information, the disclosure of which leads to damages that are not necessarily as "economic" as those resulting from the theft of credit card information and social security numbers. Indeed, Plaintiffs allege they suffered "a privacy injury by having their sensitive medical information disclosed, irrespective of whether or not they subsequently suffered identity fraud, or incurred any mitigation damages." (¶ 284.) Plus, Plaintiffs allege they noticed an increase in spam/phishing e-mails and/or calls, (¶¶ 136, 157, 192), which is harm that is also not necessarily "economic" in nature. Accordingly, at least two district court cases, with facts more similar to the instant case than those in *Dugas*, found that time spent responding to a data breach is a non-economic injury, that when alleged to support a negligence claim, defeats an economic loss doctrine argument. *See In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation*, —— F.Supp.3d ——, ——, 2020 WL 2214152, at *4 (S.D.Cal. 2020) (involving theft of medical information); *Bass*, 394 F. Supp. 3d at 1039 (involving the hack of non-financial personal information, the only alleged misuse of which was spam e-mails). Other than citing *Dugas*, Inmediata does not meaningfully address these alleged injuries in its motion to dismiss Plaintiffs' negligence claim. [11]

The applicability of the economic loss doctrine is also questionable given that Plaintiffs and Inmediata were not in privity of contract, there was no commercial activity between Plaintiffs and Inmediata that went awry, and the case does not involve a defective product or services resulting in mere "disappointed expectations." *See* *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988, 22 Cal.Rptr.3d 352, 102

P.3d 268 (2004) ("The ***914** economic loss rule requires a purchaser to recover in contract for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise. Quite simply, the economic loss rule prevents the law of contract and the law of tort from dissolving one into the other.") (internal quotation marks and alteration omitted); *see also* *Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 880 (9th Cir. 2007) (finding the economic loss doctrine did not apply because appellants' tort claim was not a "mere contract claim cloaked in the language of tort"); *Dugas*, 2016 WL 6523428, at *1 (involving dispute between parties in privity of contract).

[26] Finally, as discussed above, the statutory protection afforded to medical information is rooted in common law duties traditionally serving as the basis for lawsuits, including the duty not to publicly disclose private facts. Therefore, to the extent the economic loss rule does apply, it is plausible a common law exception to the rule also applies. (*See* Doc. No. 22 at 27-28.) Accordingly, at this stage in the litigation, the economic loss doctrine does not defeat Plaintiffs' negligence claim.

b. Duty and Breach

[27] Inmediata argues that Plaintiffs have not alleged a common law duty because "it is not plausible to suggest Inmediata could foresee that an errant web page setting would result in identity theft or fraudulent transactions using stolen patient data." (Doc. No. 17-1 at 20.) This is not an accurate description of Plaintiffs' allegations. In their FAC, Plaintiffs repeatedly, and in a variety of ways, allege that Inmediata owed them a duty to safeguard their personal and medical information as consistent with medical privacy statutes and industry standards. (¶¶ 81-87, 218-226, 231.) Emphatically, the issue here is *not* foreseeability of harm.

District courts have found comparable allegations sufficient to survive motions to dismiss negligence claims. *See* *Castillo v. Seagate Tech., LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *2 (N.D. Cal. Sept. 14, 2016) (alleging employer had duty to reasonably protect employees' information); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK, 2015 WL 3916744, at *3 (C.D. Cal. June 15, 2015) (alleging employer owed employees a duty to implement and maintain adequate security measures to safeguard their personal information); *see also* *Facebook*, 402 F. Supp. 3d at 799 (finding a duty because "Facebook had a responsibility to handle its users' sensitive information with care"); *Bass*, 394 F. Supp. 3d at 1039 (alleging Facebook failed to comply with industry data-security standards).

Inmediata cites no data breach case in which the court found the plaintiffs failed to adequately allege duty. Instead, Inmediata argues that without a "special relationship," it owed no duty to Plaintiffs to protect their information from thieves and hackers. [12] (Doc. No. 17-1 at 20.) Inmediata provides no support, however, for its argument that no special relationship exists between a company that possesses peoples' personal and medical information and those people. In *Corona*, a case upon which Inmediata relies, the court found an employer had a duty to protect the personal information it possessed regarding not only its employees and former employees, but also their spouses and dependents. 2015 WL 3916744, at *3. In reaching this conclusion, the court applied the factors identified in ***915** *Rowland v. Christian*, 69 Cal. 2d 108, 113, 70 Cal.Rptr. 97, 443 P.2d 561 (1968), which the district court described as:

> (1) the foreseeability of the harm to the plaintiff; (2) the degree of certainty that the plaintiff suffered injury; (3) the closeness of the connection between the defendant's conduct and the injury suffered; (4) the moral blame attached to the defendant's conduct; (5) the policy of preventing future harm; and (6) the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach and the availability, cost, and prevalence of insurance for the risk involved.

Id.

[28] Applied here, these factors weigh in favor of the plausibility that Inmediata owed a duty to protect Plaintiffs' information despite the fact that Plaintiffs were not Inmediata's customers or otherwise in privity with Inmediata. As noted above, Plaintiffs allege they lost time responding to Inmediata's breach notification, (¶¶ 139, 163, 195), and that they noticed an increase in spam/phishing e-mails and/or calls, (¶¶ 136, 157, 192). Plaintiffs also allege that Ms. Garcia spent her own money. (¶ 195.) It is foreseeable that these alleged harms would result from posting Plaintiffs' personal and medical information on the internet. While the chance that Plaintiffs will actually suffer identity theft is unknown [13] and has likely decreased over time, it is reasonable to infer that persons whose information was compromised in such a manner would, at the very least, spend some time and/or effort to detect or prevent identity theft. It can also reasonably be said that Inmediata bears some "moral" blame for failing to protect medical information concerning persons who were likely unaware that Inmediata possessed their medical information in the first place. (*See* ¶ 158 (alleging Mr. White spent hours "attempting to determine how he is connected to Inmediata and how his information came into the possession of Inmediata.").) Additionally, imposing a common law duty on companies that possess personal and medical information to safeguard that information further promotes a policy, statutorily recognized, of preventing identity theft and protecting the confidentiality of medical information. Finally, the burden of imposing a common law duty to protect medical and personal information is not likely high given that both state and federal law already require such protection, and, in the case of state law, already allows for a private right of action. In the context of this case, the burden appears especially light given Inmediata's position that an "errant webpage setting" was the culprit. (Doc. No. 17-1 at 20.)

Overall, it is reasonably foreseeable that a company that possesses medical information for thousands of people would cause those people time and effort upon learning that information had been freely accessible on the internet. *See* *Bass*, 394 F. Supp. 3d at 1039 (finding the *Rowland* test supported the assertion that Facebook owed its users a duty of care because, inter alia, "[t]he lack of reasonable care in the handling of personal information can foreseeably harm the individuals providing the information," including harm in the form of lost time). Accordingly, Plaintiffs plausibly allege breach of duty.

c. Causation

[29] Inmediata further argues that Plaintiffs fail to sufficiently allege causation because they do not allege an unauthorized person actually viewed or downloaded ***916** their data, or that they experienced identity theft, fraudulent charges, or any other legally cognizable harm. (Doc. No. 17-1 at 21.) The only support Inmediata provides for this argument is a citation to *Castillo*, in which the plaintiff employees all suffered identity theft in the form of falsely filed tax returns. 2016 WL 9280242, at *2. The district court found that causation was not adequately pled for one of the named plaintiffs because she conceded that her information had been compromised during a previous, unrelated data breach. *Id.* at *4. The court stated, "[t]o create a reasonable inference the [defendant's] data breach caused the [false tax] filing, [the plaintiff] should plead more particular facts connecting the two events, such as the temporal relationship between the breach and the false filing, or the similarities between the false filing in her name and the filings in the names of other [persons whose data was breached]." *Id.*

[30] This argument is persuasive with respect to the allegation that Plaintiff White actually experienced identity theft. In addition to the injuries already discussed above, Plaintiffs allege that, approximately nine months after Inmediata first learned of the data breach, Mr. White suffered $600 in fraudulent charges on his credit card. (¶¶ 159-162.) Because he used the card to pay for healthcare, Plaintiffs allege that Mr. White "believes Inmediata was the source of his breached credit card information." (¶ 162.) As was the case in *Castillo*, however, Plaintiffs acknowledge that Mr. White received a data breach notification resulting from a 2017 data breach involving Equifax. (¶ 161). Additionally, Plaintiffs acknowledge that Inmediata specifically informed them that "financial information" was "not involved." (¶ 30.) Plaintiffs nonetheless state they "do not accept this as an accurate statement" because the letter they received in

Inmediata's letter advised them to "keep[ ] a close eye on your credit card activity." (*Id.*) However, Inmediata's letter, which is attached to the FAC, contains no such language and does not reference credit card information. Additionally, Plaintiffs acknowledge that Inmediata specifically informed them "[b]ased on the investigation, we have no evidence that any files were copied or saved" and "we have not discovered any evidence that any information that may be involved in this incident has been misused." (*See* Doc. No. 16-4 at 2.) For these reasons, Plaintiffs cannot allege a plausible negligence claim based on Mr. White's allegation that he actually experienced identity theft. As discussed above, however, it is plausible the lost time and increase in spam/phishing Plaintiffs allegedly suffered was caused by the alleged breach of Inmediata's duty to protect their personal and medical information, and Inmediata does not argue otherwise.

d. Damages

i. Lost Time

[31] As noted above, Plaintiffs allege they suffered damages in the form of lost time. Specifically, Plaintiffs allege that Ms. Stasi spent time "trying to make sure she has not and does not become further victimized because of the Data Breach," (¶ 139), Mr. White spent time "dealing with the aftermath of the Data Breach," (¶ 163), and Ms. Garcia spent time "addressing issues arising from the Data Breach," (¶ 195). Plaintiffs also allege that, since early 2019 when Inmediata first became aware of the breach, they noticed an "increase in spam/phishing" e-mails, calls, or both, from "persons apparently attempting to defraud" them. (¶¶ 136, 157, 192.)

Generally, it can be inferred that theft of social security numbers, financial information, and medical information is primarily financially motivated and realized through identity theft or other forms of fraud. *See* ***917** *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."); *Bass*, 394 F. Supp. 3d at 1035 ("It is not too great a leap to assume .... that [hackers'] goal in targeting and taking .... information [is] to commit further fraud and identity theft."). Accordingly, the Ninth Circuit has held that theft of information that can be used to commit identity theft causes an injury to victims for standing purposes based on the future threat of identity theft regardless of whether the named plaintiffs actually suffered identity theft. *See* *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018), *cert. denied sub nom. Zappos.com, Inc. v. Stevens*, —— U.S. ——, 139 S. Ct. 1373, 203 L.Ed.2d 609 (2019); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010). [14]

The instant case is not, however, the typical data breach case because it does not involve the theft or hack of information that courts have recognized as enabling identity theft, such as financial information or social security numbers, and there are no plausible allegations that Plaintiffs actually suffered identity theft resulting from the alleged breach. Rather, at this stage, the case involves allegations that Plaintiffs' medical information, including diagnosis codes and treating physicians, was posted on the most publicly accessible forum in the world for an unknown period of time. In other words, the interest in the confidentiality of medical information is not, as Inmediata apparently presumes, necessarily tied to the risk of identity theft. Accordingly, although some cases have found that when information capable of being used to commit identity theft is stolen, it must also be misused in order to find injury, *see*, *e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012), the facts here are different. Although Plaintiffs do not provide great detail in describing how they expended time and effort after receiving Inmediata's breach notification, it is reasonable to infer that upon receiving notice of the breach they responded by ensuring: (1) that their medical information was no longer accessible via the internet; (2) that their information did not reappear on the internet; and/or (3) they had not, and would not, become victims of identity theft. "Increased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by other courts to be specific, concrete, and non-speculative." *Solara*, —— F.Supp.3d at ——, 2020 WL 2214152, at *4 (declining to dismiss negligence claim under Rule 12(b)(6) on this ground); *see also* *Adkins*, 424 F. Supp. 3d at 692 (time lost responding to a data breach establishes a harm for

standing purposes); *but see* *Corona*, 2015 WL 3916744, at *4 (finding, without discussion, that "general allegations of lost time are too speculative to constitute cognizable injury" in case involving an alleged hack, theft, and misuse of employee financial and medical information). It is also reasonable to infer that the receipt of alleged spam/phishing e-mails and/or calls cost ***918** Plaintiffs some of their time. Even though Plaintiffs do not allege that their e-mail addresses or phone numbers were included in the information that was compromised, it would nonetheless be reasonable for them to be curious about spam/phishing contacts they received after being informed of the data breach. *See* *Bass*, 394 F. Supp. 3d at 1035 (finding that time spent "sorting through a few dozen e-mails," though de minimis, is a sufficient injury for standing purposes because "[as] consequences of [the alleged] data breach continue to unfold, so too, will plaintiff's invested time"). Accordingly, at this early stage in litigation, Plaintiffs allege plausible damages in the form of lost time, and Inmediata has not met its burden of showing otherwise.

ii. Lost Money

[32] Plaintiffs also allege that Ms. Garcia "spent her own money .... addressing issues arising from the Data Breach." (¶ 195.) Plaintiffs do not specify what Ms. Garcia spent her money on, or what "issues" she "addressed." As pointed out by Inmediata, Plaintiffs do not allege they actually purchased credit monitoring services. (*See* Doc. No. 17-1 at 17.) Construing this allegation in the light most favorable to Plaintiffs, however, it is reasonable to infer at this stage in litigation that Ms. Garcia spent her money on some form of identity theft protection. (*See* ¶¶ 193-94 (alleging she placed credit freezes on her credit reports in order to detect potential identity theft and fraudulent activity, and now engages in monthly monitoring of her credit and her bank accounts); *see also* Doc. No. 22 at 25 ("Plaintiffs engaged credit monitoring services as a result of the .... risk of future identity theft.").)

In data breach cases involving negligence claims, district courts have found it sufficient to allege out-of-pocket expenses in purchasing identity theft protection services to show damages. *See* *Castillo*, 2016 WL 9280242, at *4 ("Those who have incurred such out-of-pocket expenses [such as purchasing identity protection services] have pleaded cognizable injuries[.]"); *Corona*, 2015 WL 3916744, at *4 (finding the same by analogizing costs associated with identity theft protection to those resulting from exposure to toxic chemicals); *see also* *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1233 (D. Nev. 2020) ("[T]angible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as damages."); *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 695 (N.D. Cal. 2019) (denying class certification because the plaintiff "never paid any money as a result of this data breach" and "never purchased any credit monitoring service"); *Yahoo*, 2017 WL 3727318, at *16 (money spent to monitor credit and prevent future identity theft is sufficient injury for standing purposes).

These cases may be distinguishable because they involve far more serious data breaches than what Plaintiffs allege here. *See* *Castillo*, 2016 WL 9280242, at *2 (defendant employer released all of its employees' tax information in response to a phishing scam, after which the plaintiff employees all suffered identity theft in the form of fraudulently filed tax returns); *Corona*, 2015 WL 3916744, at *4 (hackers stole, and traded on the internet, social security numbers, financial information, medical information, home and e-mail addresses, and visa and passport numbers). However, in arguing that Plaintiffs failed to state a claim for negligence under Rule 12(b)(6), Inmediata does not argue these cases are distinguishable. In fact, Inmediata does not specifically address the allegation that Ms. Garcia spent her own money.

Instead, Inmediata argues, as it did in its standing argument, under California law Plaintiffs' allegation that they took steps to protect against possible future ***919** risk of identity theft is insufficient.[15] (Doc. No. 17-1 at 21.) The only support Inmediata provides for this argument is a citation to *Corona*, 2015 WL 3916744. In *Corona*, however, the district court did not find that the plaintiffs failed to adequately allege injury, either for standing or Rule 12(b)(6) purposes. To the contrary, with respect to the *Corona* plaintiffs' negligence claim, the court found they adequately alleged a cognizable injury "by way of costs relating to credit monitoring, identity theft protection, and penalties." 2015

WL 3916744, at *5. Accordingly, Plaintiffs sufficiently allege that Ms. Garcia suffered damages in the form of lost money.

e. Negligence Per Se

[33] **[34]** In their FAC, Plaintiffs allege they are entitled to an evidentiary presumption of negligence per se based on violations of various statutes, including CMIA. (¶ 229.) Under California law, Inmediata's failure to exercise due care is presumed if Plaintiffs sufficiently allege that: (1) Inmediata violated a statute or regulation; (2) the violation was the proximate cause of Plaintiffs' injury; (3) the injury resulted from an occurrence, the nature of which the statute or regulation was designed to prevent; and (4) the person suffering the injury was one of the class of persons for whose protection the statute or regulation was adopted. CAL. EVID. CODE § 669. District courts have relied on allegations of negligence per se to deny Rule 12(b)(6) motions to dismiss. *See*, *e.g.*, *Harris v. Burlington N. Santa Fe R.R.*, No. EDCV 09-197 ABC (JCx), 2013 WL 12122668, at *2 (C.D. Cal. July 12, 2013). The negligence per se doctrine does not, however, obviate the need for Plaintiffs to show a viable and independent duty. *See Nikoopour v. Ocwen Loan Servicing, LLC*, Case No.: 17cv2015-MMA (WVG), 2018 WL 1035210, at *7 (S.D. Cal. Feb. 23, 2018) (citations omitted).

As discussed below, Plaintiffs plead a plausible violation of CMIA, which provides for nominal damages even if Plaintiff did not suffer actual damages. *See* CAL. CIV. CODE § 56.36(b)(1). Also, it is reasonable, at this stage in the litigation, that Plaintiffs' alleged injuries resulting from the "posting" of their medical information on the internet are the injuries the statute was intended to prevent, and that Plaintiffs, as persons who initially provided the confidential medical information that Inmediata possessed, are within the class of persons for whose protection the statute was adopted. Accordingly, to the extent the instant negligence claim is distinguishable from those in data breach cases involving a theft or hack of social security numbers or financial information, this distinction is counter-buttressed by this case involving confidential medical information protected by statute. Accordingly, the negligence per se doctrine supports the plausibility of Plaintiffs' negligence claim.

2. Breach of Contract

a. Third Party Beneficiaries

Plaintiffs allege, based on information and belief, that they are intended third party beneficiaries of contracts between Inmediata and its customers that require Inmediata to take appropriate steps to safeguard Plaintiffs' information. (¶¶ 248-49.) Inmediata argues these allegations are conclusory and not supported by any facts, such as specific contract language or the identity of the parties to the contracts. (Doc. No. 17-1 at 24-25.)

[35] The standard to achieve third party beneficiary status is a high one. *See* ***920** *Goonewardene v. ADP, LLC*, 6 Cal. 5th 817, 821, 243 Cal.Rptr.3d 299, 434 P.3d 124 (2019) (a motivating purpose of the contracting parties must be to provide a benefit to the third party); *see also* *Cummings v. Cenergy Int'l Servs., LLC*, 271 F. Supp. 3d 1182, 1188 (E.D. Cal. 2017) ("It is well settled .... that enforcement of a contract by persons who are only incidentally or remotely benefitted by it is not permitted."). Moreover, the alleged contractual terms, if they exist, likely refer to Inmediata's pre-existing statutory duties to safeguard the medical information in its possession. *See* *In re Anthem, Inc. Data Breach Litig.*, Case No. 15-MD-02617-LHK, 2016 WL 3029783, at *20 (N.D. Cal. May 27, 2016) ("A breach of contract claim based solely upon a pre-existing legal obligation to comply with HIPAA can not survive dismissal."). Additionally, district courts in data breach cases have dismissed breach of contract claims for failure to identify the specific language in the contract that was breached. *See*, *e.g.*, *Hassan v. Facebook, Inc.*, Case No. 19-cv-01003-JST, 2019 WL 3302721, at *3 (N.D. Cal. July 23, 2019).

[36] **[37]** Based on the above, Plaintiffs' breach of contract claim is tenuous at best. At this stage in the litigation, however, Plaintiffs plausibly allege they are third party beneficiaries, and Plaintiffs' allegations are sufficiently factual to give fair notice and to enable Inmediata to defend itself effectively. *See* *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). Although Plaintiffs do not provide specific contract terms, Plaintiffs allege the substance of the relevant

terms. *See* *McKell v. Washington Mut., Inc.*, 142 Cal. App. 4th 1457, 1489, 49 Cal.Rptr.3d 227 (2006); *see also* *Summit Estate, Inc. v. Cigna Healthcare of California, Inc.*, Case No. 17-CV-03871-LHK, 2017 WL 4517111, at *4 (N.D. Cal. Oct. 10, 2017). Moreover, without discovery, it is not clear what more Plaintiffs could plead, or what more Inmediata would need to be able to defend against Plaintiffs' claims that they are third party beneficiaries of Inmediata's contracts. In the early stages of litigation, plaintiffs may base their allegations, even jurisdictional ones, on information and belief when the allegations include facts that are primarily within the defendant's knowledge. *Carolina Cas. Ins. Co. v. Team Equip., Inc.*, 741 F.3d 1082, 1087 (9th Cir. 2014); *see also* *Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (*Iqbal*/*Twombly* plausibility standard does not prevent a plaintiff from pleading facts alleged upon information and belief). Accordingly, Plaintiffs' allegations that contracts exist that contain terms protecting their information are sufficient to allege a breach of contract claim based on a third party beneficiary theory.

b. Damages

Inmediata argues that Plaintiffs have not adequately pled damages because they do not plead (1) they were victims of identity theft, except for the "wildly speculative" allegations of Mr. White regarding unknown charges to his credit card, or (2) they paid for credit monitoring services. (Doc. No. 17-1 at 22.) As Inmediata points out, some district courts have found that fear of future identity theft is too speculative to support damages in a breach of contract claim. *See*, *Svenson v. Google Inc.*, 65 F. Supp. 3d 717, 724-25 (N.D. Cal. 2014); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 918 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689 (9th Cir. 2010). Additionally, the standard for damages under California contract law may be higher than that for negligence claims. *See* *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000) (plaintiffs must show appreciable and actual damage that is not nominal, speculative, or based on fear of future harm). Also, as discussed above, Inmediata is correct that Mr. White's allegations regarding the fraudulent charges on his credit card are unreasonably speculative.

***921** **[38]** However, the cases dismissing breach of contract claims for lack of plausible damages did not involve medical information that was allegedly posted on the internet. Moreover, Inmediata does not argue that breach of contract claims have substantively different standards for damages than negligence claims. Also, Inmediata is incorrect that Plaintiffs' fail to allege they paid for credit monitoring services. Rather, as discussed above, Plaintiffs allege that Ms. Garcia "spent her own money .... addressing issues arising from the Data Breach," (¶ 195), and this is sufficient to infer that she spent the money on some form of identity theft protection.

Additionally, other district courts have found, or at least suggested, that an alleged invasion of privacy is per se sufficient to show damages in a breach of contract claim. *See* *Facebook*, 402 F. Supp. 3d at 802 ("[U]nder California law even those plaintiffs [who did not suffer measurable compensatory damages] may recover nominal damages."); *Solara*, —— F.Supp.3d at ——, 2020 WL 2214152, at *5 ("The dissemination of one's personal information can satisfy the damages element of a breach of contract claim."); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 834 (N.D. Cal. 2020) ("[T]he detriment Plaintiffs say they suffered was an invasion of their privacy. Plaintiffs are entitled to seek compensatory damages or perhaps nominal damages for such harm."); *see also* *Facebook Tracking*, 956 F.3d 589, 598 (9th Cir. 2020) (finding that plaintiffs had standing to bring claims for breach of contract by adequately alleging "privacy harms"). Accordingly, Plaintiffs sufficiently plead damages in their breach of contract claim.

3. Unjust Enrichment

[39] Inmediata argues, and Plaintiffs concede, that they have not pled a plausible claim for unjust enrichment under California law. (*See* Doc. Nos. 17-1 at 24-25; 22 at 30 n.2.) Accordingly, Plaintiffs fail to state a plausible claim for unjust enrichment under California law. Plaintiffs nonetheless argue that Inmediata does not challenge their unjust enrichment claims under Florida and Minnesota law. (Doc. No. 22 at 30.) In their FAC, however, Plaintiffs do not list their purported claims for unjust enrichment under Florida or Minnesota law as separate claims, and Plaintiffs make only passing

reference to Florida and Minnesota law. (*See* ¶¶ 226-27.) To the extent that Plaintiffs actually and sufficiently allege unjust enrichment under Florida and Minnesota law, those claims survive because they are not challenged.

4. California Confidentiality of Medical Information Act

Inmediata argues that Plaintiffs fail to state a plausible violation of CMIA, CAL. CIV. CODE §§ 56-56.265, because they do not allege facts suggesting that an unauthorized person "actually viewed" their confidential information. (Doc. No. 17-1 at 26.) As noted above, Plaintiffs allege that by posting their medical information on the internet, Inmediata violated multiple provisions of CMIA, including the first sentence of section 56.10(a) (prohibiting "disclosure"), the first sentence of section 56.101(a) (establishing a duty to "preserve confidentiality"), and section 56.36(b) (allowing a private right of action for "negligent release"). [16] (¶¶ 269-71, 277.) As a result, Plaintiffs seek actual and nominal damages. (¶ 281.)

*922 a. Section 56.10(a)

[40] Under California law, in order to plead a violation of section 56.10(a), which mandates that health care providers and contractors shall not "disclose" medical information, the plaintiff must plead an "affirmative communicative act" by the defendant, which does not occur if the information is stolen. *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1556, 174 Cal.Rptr.3d 653 (2014); *see also* *Regents of Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 564, 163 Cal.Rptr.3d 205 (2013) ("disclose" under CMIA means an "affirmative act of communication"). Plaintiffs allege that Inmediata employees "posted" their information on the internet, and that "posting" is an affirmative communicative act. (¶¶ 269-71.)

[41] Here, it is reasonable to infer that some affirmative act by Inmediata caused the "errant webpage setting" that allegedly made Plaintiffs' information accessible via the internet. However, while intentionally posting something on the internet is inherently communicative, Plaintiffs do not allege that Inmediata intentionally [17] posted their information, or that whatever affirmative act might have caused their information to become accessible via the internet was done with the intent to communicate that information. Based on the meaning of "disclose" as defined in *Sutter* and *Regents*, Plaintiffs have not pled a plausible violation of section 56.10(a) of CMIA.

b. Sections 56.101(a) and 56.36(b)

[42] The first sentence of section 56.101(a) in CMIA provides that every health care provider and contractor "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." [18] CAL. CIV. CODE § 55.101(a). The second sentence provides that any health care provider or contractor "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Section 56.36(b) provides, in turn, that nominal and actual damages are available when information is "negligently released." [19] § 56.36(b). In *Regents*, the court ***923** held that in order to plead a violation of sections 56.101(a) and 56.36(b), the plaintiff does *not* need to plead an affirmative communicative act. 220 Cal. App. 4th at 553-54, 163 Cal.Rptr.3d 205; *see also* *Corona*, 2015 WL 3916744, at *7; *Sutter*, 227 Cal. App. 4th at 1554, 174 Cal.Rptr.3d 653 (assuming the same). The court also held, however, that plaintiffs must plead that "negligence result[ed] in unauthorized or wrongful access to the information," i.e. that the information was "improperly viewed or otherwise accessed." [20] *Id.* at 554, 163 Cal.Rptr.3d 205. Similarly, in *Sutter*, the court held that "[n]o breach of confidentiality takes place until an unauthorized person views the medical information." 227 Cal. App. 4th at 1557, 174 Cal.Rptr.3d 653. The *Sutter* court stated, "[t]hat the records have changed possession even in an unauthorized manner does not mean they have been

exposed to the view of an unauthorized person." *Id.* at 1558, 174 Cal.Rptr.3d 653.

[43] Here, *Regents* and *Sutter* do not preclude Plaintiffs' remaining CMIA claims because the Plaintiffs repeatedly allege their information "was viewed by unauthorized persons."[21] (¶¶ 269-271, 277.) The lack of allegations that the plaintiffs' information was actually viewed was crucial to the courts' decisions in *Regents* and *Sutter*. *See* *Sutter*, 227 Cal. App. 4th at 1555, 174 Cal.Rptr.3d 653 ("[T]he main pleading problem for the plaintiffs in this case and in *Regents* is the same: there is no allegation that the medical information was viewed by an unauthorized person."). Additionally, in both *Regents* and *Sutter*, the stolen data was password protected and/or encrypted. *See* *Sutter*, 227 Cal. App. 4th at 1555, 174 Cal.Rptr.3d 653. The same cannot be said for information that is posted and accessible on the internet.[22] Given the relatively clear holdings in *Regents* and *Sutter*, Plaintiffs' allegation that their information was actually viewed could be read, of course, as a threadbare and conclusory recital of an essential element to their CMIA claim. When read in the light most favorable to Plaintiffs, however, the allegation that their information was actually viewed is at least somewhat factual.

Additionally, one court in this district recently found it sufficient for plaintiffs to plead that they received a letter stating their medical information was exposed in a data breach, and the only evidence that it ***924** had actually been viewed was an increase in medical-related spam e-mails and phone calls. *See* *Solara*, —— F.Supp.3d at ——, 2020 WL 2214152, at *7. The court found these allegations sufficient to infer the plaintiffs' medical information was viewed by an unauthorized party, even though the plaintiffs did not specifically allege that it was. *Id.* As an alternative to their allegation that their information was actually viewed, Plaintiffs repeatedly assert that they reasonably believe, and it should be inferred or rebuttably presumed, that their information was actually viewed. (*See*, *e.g.*, ¶¶ 46-48.) Given that Plaintiffs allege that Inmediata posted their information on the internet, making it searchable, findable, viewable, printable, copiable, and downloadable by anyone in the world with an internet connection, (¶¶ 7-8), it can be reasonably inferred that someone viewed it. Ultimately, it may be that Plaintiffs' allegation that their information was actually viewed while it was accessible on the internet will prove to be unsubstantiated. At this early stage in the litigation, however, Plaintiffs allege a plausible claim based on violations of sections 56.101(a) and 56.36(b) of CMIA, and Inmediata has not met its burden of showing otherwise.

5. California Consumer Privacy Act

[44] Inmediata argues that Plaintiffs fail to state a claim for violation of the California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.150(a), because (1) Plaintiffs merely allege that it should be inferred or rebuttably presumed that their information was accessed by an unauthorized individual, which is insufficient to allege theft of or "unauthorized access" to their personal information, and (2) Plaintiffs allege violation of the CCPA based on the exposure of both their personal and medical information, but the CCPA does not apply to medical information governed by CMIA. (Doc. No. 17-1 at 27.)

As discussed above, Plaintiffs do not merely allege that it should be inferred or rebuttably presumed that their information was accessed by an unauthorized individual. Plaintiffs repeatedly allege that their information "was viewed by unauthorized persons." (*See*, *e.g.*, ¶¶ 269-271, 277.) Moreover, Inmediata does not point to any authority requiring Plaintiffs to plead theft or unauthorized access in order to plead a plausible violation of the CCPA. The CCPA provides a private right of action for actual or statutory damages to "[a]ny consumer whose nonencrypted and nonredacted personal information .... 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[.]" *Id.* § 1798.150(a). Plaintiffs argue, and Inmediata does not dispute, that the facts alleged in the FAC that Plaintiffs' personal and medical information were accessible via the internet, constitutes a "disclosure" under the CCPA. (Doc. No. 22 at 22-23.) Further, although Inmediata is correct that the CCPA does not apply to medical information governed by CMIA, § 1798.145(c)(1)(A), Inmediata does not address

the non-medical information that it admits was accessible on the internet. Accordingly, at this early stage in the litigation, Plaintiffs allege a plausible claim based on violation of the CCPA, and Inmediata has not met its burden of showing otherwise.

6. California Consumer Records Act

[45] Plaintiffs allege that by taking 81 days to inform them of the data breach, Inmediata acted with unreasonable delay in violation of the California Customer Records Act (CCRA), CAL. CIV. CODE § 1798.82(a). (¶ 297.) Inmediata argues that Plaintiffs allege no facts demonstrating unreasonable ***925** delay in notifying them of the alleged breach, and therefore, Plaintiffs fail to state a CCRA violation. (Doc. No. 17-1 at 28.) Inmediata further argues that Plaintiffs did not allege harm or subsequent incremental harm from the delay. (*Id.*)

The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California .... whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person .... in the most expedient time possible and without unreasonable delay[.]" CAL. CIV. CODE § 1798.82(a).

Inmediata cites no authority to support its argument that 81 days is reasonable delay. Additionally, the only authority Inmediata cites to support its argument that Plaintiffs are required to allege harm or incremental harm from the delay is *Yahoo*, 2017 WL 3727318, at *41. In *Yahoo*, however, the court found the plaintiffs adequately alleged incremental harm by alleging that, if they had been notified earlier, they could have taken steps to mitigate the "fallout" from their information being stolen. *Id.* Similarly, Plaintiffs allege that because of the delay they were "prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze." (¶ 301.) Plaintiffs also allege these measures could have prevented some of their damages because their information would have been less valuable to identity thieves. (*Id.*) Although only one Plaintiff, Mr. White, allegedly experienced "fallout" in the form of identity theft, Inmediata does not specifically address Plaintiffs' allegations regarding their incremental harm. Instead, Inmediata argues, inaccurately, that "Plaintiffs here have not alleged harm or subsequent 'incremental harm' from delay." (Doc. No. 17-1 at 28.) Accordingly, at this early stage in the litigation, Plaintiffs allege a plausible claim based on violations of the CCRA, and Inmediata has not met its burden of showing otherwise.

7. Minnesota Health Records Act

[46] Plaintiffs allege that Inmediata violated the Minnesota Health Records Act (MHRA), MINN. STAT. ANN. §§ 144.29-144.34, by releasing their health records without first obtaining consent or authorization, and by negligently or intentionally releasing their health records. (¶¶ 312-13.) Inmediata argues these allegations are conclusory and not supported by factual allegations. (Doc. No. 17-1 at 28-29.) Inmediata also argues this claim should be dismissed because "Plaintiffs did not and cannot allege facts suggesting that any unauthorized person actually searched for, found, viewed, or downloaded the data at issue." (*Id.* at 29.) As discussed above, however, Plaintiffs allege that Inmediata posted their medical information on the internet for an unknown period of time. Additionally, Plaintiffs repeatedly allege that their information was viewed. Inmediata also provides no support for its argument that by posting medical information on the internet, where it was allegedly viewed, is insufficient to plead a plausible claim under the MHRA. Accordingly, at this early stage in the litigation, Plaintiffs allege a plausible claim based on violations of the MHRA, and Inmediata has not met its burden of showing otherwise.

8. Article I, Section 1 of the California Constitution

[47] **[48]** Finally, Inmediata argues that Plaintiffs' claim under the California Constitution it was not Inmediata.[23] (Doc. No. ***926** 17-1 at 29-30.) The California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. I, § 1. The parties

do not dispute that to support a claim under this provision, Plaintiffs must show: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 39-40, 26 Cal.Rptr.2d 834, 865 P.2d 633 (1994). The parties also do not dispute that Plaintiffs have a legally protected privacy interest in their medical information. *See also Heldt v. Guardian Life Ins. Co. of Am.*, Case No. 16-cv-885-BAS-NLS, 2019 WL 651503, at *4 (S.D. Cal. Feb. 15, 2019) (recognizing a legally protected privacy interest in medical information held by an insurer).

[49] Whether Plaintiffs had a reasonable expectation of privacy, and whether Inmediata's conduct constitutes a serious invasion of privacy, are mixed questions of law and fact. *See Hill*, 7 Cal. 4th at 40, 26 Cal.Rptr.2d 834, 865 P.2d 633; *see also Facebook Tracking*, 956 F.3d at 606 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."). At this stage in the litigation, it is reasonable to infer that Plaintiffs reasonably expected Inmediata would not post their medical information on the internet, negligently or otherwise, and that doing so constitutes a serious invasion of privacy. Although some courts have dismissed privacy claims based on the state constitution given the "high bar" for such claims, *see Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (listing cases), these cases do not involve medical information that was "posted" on the internet, *see Hill*, 7 Cal. 4th at 35, 26 Cal.Rptr.2d 834, 865 P.2d 633 ("Legally recognized privacy interests [include] interests in precluding the dissemination or misuse of sensitive and confidential information."); *Strawn v. Morris, Polich & Purdy, LLP*, 30 Cal. App. 5th 1087, 1100, 242 Cal.Rptr.3d 216 (2019) (finding the seriousness of the alleged invasion of privacy based on disclosure of plaintiffs' tax returns presented a question of fact that could not be resolved on demurrer). Moreover, Inmediata provides no support for its argument that negligently posting medical information on the internet does not constitute a serious invasion of privacy, and only those who hack or steal information can be held liable. *See Doe v. Beard*, 63 F. Supp. 3d 1159, 1170 (C.D. Cal. 2014) (negligent disclosure of plaintiff's medical information was sufficient to sustain a breach of privacy claim under the state constitution); *but see Razuki v. Caliber Home Loans, Inc.*, Case No. 17cv1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (suggesting the conduct must be intentional). Accordingly, at this early stage in litigation, Plaintiffs allege a plausible violation of the state constitution's privacy provision, and Inmediata has not met its burden of showing otherwise.

IV. CONCLUSION

For the foregoing reasons, Inmediata's Motion to Dismiss under Rule 12(b)(1) for lack of standing is **DENIED**. Inmediata's Motion to Dismiss under Rule 12(b)(6) is **DENIED IN PART** and **GRANTED IN PART**. Inmediata's Motion to Dismiss Plaintiffs' claims for negligence, breach of contract, violation of sections 56.101(a) and 56.36(b) of CMIA, as well as violations of ***927** the CCPA, CCRA, MHRA, and the California Constitution, is **DENIED**. Inmediata's Motion to Dismiss Plaintiffs' claims for unjust enrichment and violation of section 56.10(a) of CMIA is **GRANTED**. In their opposition to the instant motion, Plaintiffs do not request leave to amend. Inmediata's answer to the operative complaint is due ***within 21 days*** of this court's order.

IT IS SO ORDERED.

All Citations

501 F.Supp.3d 898

Footnotes

1 Well pled allegations of the FAC are taken as true for purposes of ruling on the motion before the court.

2 Citations to "¶" refer to the FAC.

3 Other than citing *Spokeo II*, Plaintiffs provide almost no support for their statutory standing argument. Plaintiffs do not, for example, discuss the CMIA or its legislative history. Notwithstanding these omissions, the court has an independent obligation to assure Plaintiffs' Article III standing. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180, 120 S.Ct. 693, 145 L.Ed.2d 610 (2000).

4 The CMIA applies to health care providers, service plans, and contractors. CAL. CIV. CODE § 56.10(a). Inmediata does not dispute that it is subject to the CMIA.

5 Plaintiffs do not provide a definition as to what "posting" information on the internet entails. As discussed below, it is not reasonable to infer that Inmediata intentionally posted Plaintiffs' information on the internet. Interpreting the "posting" term in the light most favorable to Plaintiffs, it means that information was made accessible to anyone with an internet connection, intentionally or not.

6 In *Spokeo*, the Supreme Court emphasized that "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." 136 S. Ct. at 1549. The Court also emphasized, however, that the violation of a statutory right, even a procedural one, "can be sufficient in some circumstances to constitute injury in fact." *Id.* In such cases, "a plaintiff .... need not allege any additional harm beyond the one Congress has identified." *Id.*

7 Although in *Spokeo* the Supreme Court examined the judgment of Congress "because Congress is well positioned to identify intangible harms that meet minimum Article III requirements, 136 S. Ct. at 1549, the Ninth Circuit has applied this line of inquiry to state legislatures and state statutes. *See* *Facebook Tracking*, 956 F.3d at 598 ("[H]istory and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights[.]"); *Campbell*, 951 F.3d at 1116 ("[W]e are guided in determining concreteness by 'both history and the judgment of Congress,' or the legislature that enacted the statute."); *Patel*, 932 F.3d at 1273 ("The judgment of the Illinois General Assembly .... is 'instructive and important' to our standing inquiry[.]").

8 Because injury in fact exists based on an alleged violation of CMIA, it is not necessary to address Plaintiffs' argument that they also possess standing based on violation of the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1302d.

9 Courts have consistently found, with little or no discussion, that concrete injuries based on violations of privacy-related statutes are also particularized, fairly traceable (to Inmediata, in this case), and likely to be redressed by a favorable decision. *See*, *e.g.*, *Campbell*, 951 F.3d at 1116 n.7; *see also* *Dutta v. State Farm Mut. Auto. Ins. Co.*, 895 F.3d 1166, 1173 (9th Cir. 2018) (injury in fact is the "first and foremost element" of standing). Here, there is no other source of the alleged injury than Inmediata, and the allege injury to Plaintiffs could be redressed by an award of damages or other relief. Also, Inmediata's standing argument does not rest on traceability or redressability issues. Accordingly, Plaintiffs have met their burden of adequately pleading all the elements of standing.

10 For the same reasons as those stated in the court's initial order granting Inmediata's motion to dismiss, (Doc. No. 15), Plaintiffs arguments with respect to injury based on the future risk of identity theft are unavailing.

11 In its reply, Inmediata merely states, without citing any authority, that "the loss of time does not meet the requirement that there must be bodily injury or property damage." (Doc. No. 23 at 11.)

12 For this reason, Inmediata's argument concerning a common law duty appears to be aimed more towards Inmediata's economic loss doctrine argument rather than attacking the duty element of Plaintiffs' negligence claim.

13 As discussed below, it is also far from reasonably certain Mr. White's alleged identity theft was the result of this data breach.

14 As this court previously found, in both *Krottner* and *Zappos* the Ninth Circuit held that misuse of the named plaintiffs' information was not necessarily required for standing purposes, but the court nonetheless relied on allegations of actual misuse of others victims' information to find standing. *See* *Krottner*, 628 F.3d at 1142 (noting that one of the plaintiffs alleged that someone unsuccessfully attempted to open a bank account in his name); *Zappos*, 888 F.3d at 1027-28 (noting that some non-parties had their accounts commandeered and suffered financial losses, and that two plaintiffs had their e-mail accounts taken over).

15 Inmediata's reference to its argument against Plaintiffs' standing in support of its argument against Plaintiffs' negligence claims is not particularly helpful given that Plaintiffs bear the burden of showing standing while Inmediata bears the burden of showing that Plaintiffs failed to state their claim for negligence under Rule 12(b)(6).

16 Plaintiffs also allege that Inmediata violated: (1) sections 56.101(b)(1) related to its electronic health record system; (2) section 56.26(a) by using their information in a manner not reasonably necessary in connection with the administration or maintenance of payment for health care services program; (3) section 56.10(d) by intentionally using their information for a purpose not necessary to provide health care services; and (4) section 56.10(e) by disclosing their information to persons or entities not engaged in providing direct health care services. (¶273-276, 278-79.) Inmediata does not argue that Plaintiffs have failed to state a claim with respect to these provisions.

17 Although Plaintiffs allege that Inmediata "intentionally shared, sold, used for marketing, or otherwise used" their information "for a purpose not necessary to provide health care services," (¶ 278), this is merely a recitation of the elements of section 56.10(d) of the CMIA. The same is true where Plaintiffs use the word "intent" to allege fraud. (See ¶ 304.)

18 Unlike other provisions of the CMIA, however, this provision does not state that damages are available for violations. *See* *Lu v. Hawaiian Gardens Casino, Inc.*, 50 Cal. 4th 592, 596, 113 Cal.Rptr.3d 498, 236 P.3d 346 (2010) ("A violation of a state statute does not necessarily give rise to a private cause of action."). As recognized in *Regents*, to allow claims based on violation of this provision alone would allow persons other than the patient to bring suit. *Regents*, 220 Cal. App. 4th at 563, 163 Cal.Rptr.3d 205.

19 On its face, the statute is unclear as to whether, in order to recover actual or nominal damages for, say, "negligent maintenance" of information, the plaintiff must also show that the information was "negligently released." In *Regents*, however, the court clarified that in order to sufficiently plead actual or nominal damages under CMIA, it is insufficient for the plaintiff to plead, under the second sentence of section 56.101(a), that the defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information. 220 Cal. App. 4th at 554, 163 Cal.Rptr.3d 205. Rather, the plaintiff must also plead that their information was negligently "released" under section 56.36(b). *Id.*

20 The court found that pleading negligent maintenance and loss of possession based on the theft of the data is insufficient to state a claim under sections 56.101 and 56.36(b). *Regents*, 220 Cal. App. 4th at 569-70, 163 Cal.Rptr.3d 205.

21 Strangely, Inmediata argues that "Plaintiffs do not even allege an unauthorized person actually viewed or downloaded their data." (Doc. No. 17-1 at 21.)

22 In cases where the plaintiffs allege their information was stolen and actually misused, district courts have declined to dismiss CMIA claims under Rule 12(b)(6). *See* *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1202 (D. Or. 2016) (hack); *Corona*, 2015 WL 3916744, at *7 (hack); *Falkenberg v. Alere Home Monitoring, Inc.*, Case No. 13-cv-00341-JST, 2015 WL 800378, at *4 (N.D. Cal. Feb. 23, 2015) (theft of a password protected laptop). Here, only one of the Plaintiffs alleges actual identity theft, and it is a weak allegation at that. This weakness is counter-balanced, however, because the Plaintiffs information was allegedly accessible on the most public forum in the world, and not just to the thief or thieves. And again, Inmediata does not argue to any convincing degree that cases involving theft or hacking are distinguishable. Additionally, when suing for nominal damages under CMIA, plaintiffs do not have to prove they "suffered or [were] threatened with actual damages." CAL. CIV. CODE § 56.36(b)(1).

23 Although Plaintiffs allege both invasion of privacy and violation of the California Constitution, (¶ 319), Inmediata does not move to dismiss Plaintiffs' invasion of privacy claim.

End of Document

EXHIBIT 8

2021 WL 3568394
Only the Westlaw citation is currently available.
United States District Court, D.
South Carolina, Columbia Division.

IN RE: BLACKBAUD, INC., CUSTOMER DATA BREACH LITIGATION

Case No. 3:20-mn-02972-JMC
|
MDL No. 2972
|
Signed 08/12/2021

THIS DOCUMENT RELATES TO: ALL ACTIONS:

ORDER AND OPINION

J. Michelle Childs, United States District Judge

This matter is before the court on Defendant Blackbaud, Inc.'s ("Blackbaud") Motion to Dismiss seven (7) of Plaintiffs' statutory claims pursuant to Federal Rule of Civil Procedure 12(b)(6). (ECF No. 110.) For the reasons set forth below, the court **GRANTS IN PART** and **DENIES IN PART** Blackbaud's Motion. (*Id.*)

I. RELEVANT BACKGROUND

Blackbaud is a publicly traded cloud software company incorporated in Delaware and headquartered in Charleston, South Carolina. (ECF No. 77 at 110-11 ¶ 419, 112 ¶ 424.) The company provides data collection and maintenance software solutions for administration, fundraising, marketing, and analytics to social good entities such as non-profit organizations, foundations, educational institutions, faith communities, and healthcare organizations ("Social Good Entities"). (*Id.* at 4 ¶ 4, 114 ¶ 430.) Blackbaud's services include collecting and storing Personally Identifiable Information ("PII") and Protected Health Information ("PHI") from its customers' donors, patients, students, and congregants. (*Id.* at 3 ¶ 2, 114 ¶ 429.)

In this action, Plaintiffs represent a putative class of individuals whose data was provided to Blackbaud's customers and managed by Blackbaud. (*Id.* at 6 ¶ 12.) Thus, Plaintiffs are patrons of Blackbaud's customers rather than direct customers of Blackbaud. (ECF Nos. 92-1 at 9; 109 at 7-8.)

Plaintiffs assert that from February 7, 2020 to May 20, 2020, cybercriminals orchestrated a two-part ransomware attack on Blackbaud's systems ("Ransomware Attack"). (ECF No. 77 at 11-12 ¶ 25.) Cybercriminals first infiltrated Blackbaud's computer networks, copied Plaintiffs' data, and held it for ransom. (*Id.* at 11 ¶ 25, 137 ¶ 496; ECF No. 92-1 at 7.) When the Ransomware Attack was discovered in May 2020, the cybercriminals then attempted but failed to block Blackbaud from accessing its own systems. (*Id.*) Blackbaud ultimately paid the ransom in an undisclosed amount of Bitcoin in exchange for a commitment that any data previously accessed by the cybercriminals was permanently destroyed. (ECF Nos. 77 at 9 ¶ 20, 138 ¶ 499; 92-1 at 7.)

Plaintiffs maintain that the Ransomware Attack resulted from Blackbaud's "deficient security program[.]" (ECF No. 77 at 117-18 ¶ 439.) They assert that Blackbaud failed to comply with industry and regulatory standards by neglecting to implement security measures to mitigate the risk of unauthorized access, utilizing outdated servers, storing obsolete data, and maintaining unencrypted data fields. (*Id.* at 117-18 ¶ 439, 134 ¶ 486, 136 ¶ 491, 142 ¶ 510.)

Plaintiffs further allege that after the Ransomware Attack, Blackbaud launched a narrow internal investigation into the attack that analyzed a limited number of Blackbaud systems and did not address the full scope of the attack. (*Id.* at 143 ¶ 514.) On July 14, 2020, Blackbaud received the investigation report ("Forensic Report") which acknowledged that "names, addresses, phone numbers, email addresses, dates of birth, and/or SSNs" were disclosed in the breach but stated that the investigation was "unable to detect credit card data while reviewing exfiltrated data[.]" (*Id.* at 143 ¶ 514 n.112, 144 ¶ 516, 154 ¶ 549.) Plaintiffs claim the Forensic Report "improperly concludes that no credit card data was exfiltrated" because "such data could have existed in the unexamined database files." (*Id.* at 144 ¶ 516.)

***2** Plaintiffs contend that Blackbaud failed to provide them with timely and adequate notice of the Ransomware Attack and the extent of the resulting data breach. (*Id.* at 130-31 ¶ 473.) They claim that they did not receive notice of the Ransomware Attack "until July of 2020 at the earliest[.]" (*Id.* at 156 ¶ 555.) On July 16, 2020, The NonProfit Times reported that Blackbaud had been the subject of a ransomware attack and data breach and Blackbaud issued a statement about the Ransomware Attack on its website. (*Id.* at 9 ¶ 20, 138 ¶ 499.) In both disclosures, Blackbaud asserted that the cybercriminals did not access credit card information, bank account information, or SSNs. (*Id.*)

Plaintiffs allege that they subsequently received notices of the Ransomware Attack from various Blackbaud customers at different points in time from July 2020 to January 2021. (*See, e.g.*, *id.* at 25 ¶ 63, 29 ¶ 82, 32 ¶ 93, 109 ¶ 414.) They maintain that some of the notices stated that SSNs, credit card data, and bank account information were not accessed during the Ransomware Attack while others stated that SSNs but not credit card data or bank account information were exposed during the Ransomware Attack. (*See, e.g.*, *id.* at 25 ¶ 64, 29 ¶ 82, 52 ¶ 173, 65 ¶ 230.)

Plaintiffs maintain that although Blackbaud initially represented that sensitive information such as SSNs and bank account numbers were not compromised in the Ransomware Attack, Blackbaud informed certain customers in September and October 2020 that SSNs and other sensitive data were in fact stolen in the breach. (*Id.* at 141-42 ¶ 509.) Additionally, on September 29, 2020, Blackbaud filed a Form 8-K with the Securities and Exchange Commission stating that SSNs, bank account information, usernames, and passwords may have been exfiltrated during the Ransomware Attack. (*Id.* at 12 ¶ 26, 143 ¶ 512.)

After the Ransomware Attack was made public, putative class actions arising out of the intrusion into Blackbaud's systems and subsequent data breach were filed in state and federal courts across the country. (ECF No. 1 at 1.) On December 15, 2020, the Judicial Panel on Multidistrict Litigation consolidated all federal litigation related to the Ransomware Attack into this multidistrict litigation ("MDL") for coordinated pretrial proceedings. [1] (*Id.* at 3.)

On April 2, 2021, thirty-four (34) named Plaintiffs [2] from twenty (20) states filed a Consolidated Class Action Complaint ("CCAC") alleging that their PII and/or PHI was compromised during the Ransomware Attack. (ECF No. 77.) [3] They assert six (6) claims on behalf of a putative nationwide class as well as ninety-one (91) statutory claims on behalf of putative state subclasses. (*Id.* at 173 ¶ 627 – 424 ¶ 1815.)

To facilitate the efficient resolution of the litigation, the court ordered that the first phase of motions practice address jurisdictional issues, certain statutory claims, and specific common law claims. (ECF Nos. 23 at 2; 78 at 1.) On May 3, 2021, Blackbaud filed a Motion to Dismiss for Lack of Subject Matter Jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1) ("Jurisdictional Motion to Dismiss"). (ECF No. 92.) The court denied Blackbaud's Jurisdictional Motion to Dismiss on July 1, 2021. (ECF No. 121.)

***3** Blackbaud filed the instant Motion to Dismiss pursuant to Rule 12(b)(6) on June 4, 2021, contending that Plaintiffs' California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code §§ 1798.100–1798.199.95; California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §§ 56–56.265; Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201–501.213; New Jersey Consumer Fraud Act ("NJCFA"), N.J. Stat. Ann. §§ 56:8-1–56:8-20; New York General Business Law ("GBL") § 349; Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 P.S. §§ 201-1–201-9.2; and South Carolina Data Breach Security Act ("SCDBA"), S.C. Code Ann. § 39-1-90, claims (collectively, "Select Statutory Claims") should be dismissed for failure to state a claim. (ECF No. 110.) Plaintiffs filed a Response on July 6, 2021. (ECF No. 123.) The court held a hearing on the Motion on July 20, 2021. (ECF Nos. 136, 137.)

II. LEGAL STANDARD

A. Applicable Law

In federal diversity actions, federal law governs procedural issues and state law governs substantive issues. *See* *Dixon v. Edwards*, 290 F.3d 699, 710 (4th Cir. 2002). In the MDL context, a transferee court must apply federal law as

interpreted by the circuit where the transferee court sits to matters of procedure. *See, e.g.*, *In re Porsche Cars North America, Inc.*, 880 F. Supp. 2d 801, 815 (S.D. Ohio 2012); *McGuffie v. Mead Corp.*, 733 F. Supp. 2d 592, 594 (E.D. Pa. 2010). Accordingly, the court will apply the United States Court of Appeals for the Fourth Circuit's interpretation of federal procedural law. In contrast, the court "must apply the jurisprudence of the relevant state's highest court or, if it has not spoken to the issue, predict how the state's highest court would rule" to analyze Plaintiffs' state statutory claims. *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 467 (D. Md. 2020) (citing *Erie Railroad Co. v. Tompkins*, 304 U.S. 64, 58 (1938); *Private Mortg. Inv. Servs., Inc. v. Hotel & Club Assocs., Inc.*, 296 F.3d 308, 312 (4th Cir. 2002)).

B. Motion to Dismiss

A motion to dismiss pursuant to Rule 12(b)(6) "challenges the legal sufficiency of a complaint." *Francis v. Giacomelli*, 588 F.3d 186, 192 (4th Cir. 2009). It is not intended to " 'resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses.' " *Presley v. City of Charlottesville*, 464 F.3d 480, 483 (4th Cir. 2006) (quoting *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999)).

A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Thus, "[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (quoting *Twombly*, 550 U.S. at 556). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (citing *Twombly*, 550 U.S. at 556).

When considering a Rule 12(b)(6) motion to dismiss, the court must accept all well-pled factual allegations as true and view the complaint in the light most favorable to the plaintiff. *See e.g.*, *Aziz v. Alcolac*, 658 F.3d 388, 391 (4th Cir. 2011); *Ostrzenski v. Seigel*, 177 F.3d 245, 251 (4th Cir. 1999). However, the court is not required to accept legal conclusions as true. *Aziz*, 658 F.3d at 391 (citing *Iqbal*, 556 U.S. at 680).

***4** To survive a motion to dismiss, "claims of fraud" must satisfy both Rule 8(a)'s plausibility requirement and Federal Rule of Civil Procedure 9(b)'s particularity standard. *Xia Bi v. McAuliffe*, 927 F.3d 177, 182 (4th Cir. 2019). Rule 9(b) imposes a heightened pleading standard on fraud claims, requiring a plaintiff to "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). The Rule 9(b) particularity standard requires a party to, "at a minimum, describe 'the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby.' These facts are often 'referred to as the who, what, when, where, and how of the alleged fraud.' " *Bakery & Confectionary Union & Indus. Int'l Pension Fund v. Just Born II, Inc.*, 888 F.3d 696, 705 (4th Cir. 2018) (quoting *U.S. ex rel. Wilson v. Kellogg Brown & Root, Inc.*, 525 F.3d 370, 379 (4th Cir. 2008)). Rule 9(b)'s heightened pleading requirements apply to state law claims litigated in federal court. *Topshelf Mgmt., Inc. v. Campbell-Ewald Co.*, 117 F. Supp. 3d 722, 726 (M.D.N.C. 2015) (citing *U.S. ex rel. Palmieri v. Alpharma, Inc.*, 928 F. Supp. 2d 840, 853 (D. Md. 2013)).

As the court will decide the instant Motion to Dismiss before class certification, the court's rulings will only bind the named Plaintiffs. MANUAL FOR COMPLEX LITIGATION (FOURTH) § 21.11 (2004) ("Motions such as challenges to jurisdiction and venue, motions to dismiss for failure to state a claim, and motions for summary judgment may be decided before a motion to certify the class, although such precertification rulings bind only the named parties.").

III. ANALYSIS

Blackbaud contends that the court should dismiss Plaintiffs' Select Statutory Claims for failure to state a claim. (ECF No. 110 at 10.) The court will address each claim in turn.

A. California Consumer Privacy Act Claims

California Plaintiffs Kassandre Clayton ("Clayton"), Philip Eisen ("Eisen"), Mamie Estes ("Estes"), and Shawn Regan ("Regan") (collectively, "California Plaintiffs") allege claims under the CCPA. (ECF No. 77 at 214 ¶ 819 – 216 ¶ 833.) The CCPA

> provides a private right of action for actual or statutory damages to "[a]ny consumer whose nonencrypted and nonredacted personal information ... 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[.]"

Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020) (quoting Cal. Civ. Code § 1798.150(a) (West 2021)) (emphasis added). Blackbaud contends California Plaintiffs' CCPA claims fail as a matter of law because Blackbaud is not a "business" regulated by the Act. (ECF No. 110-1 at 19.)

Since the CCPA only applies to data breaches that occurred after January 1, 2020, courts have had few opportunities to dissect the Act's provisions. *See Gardiner v. Walmart Inc.*, No. 20-CV-04618-JSW, 2021 WL 2520103, at *2 (N.D. Cal. Mar. 5, 2021) (finding that data breaches are only actionable under the CCPA if they occur after January 1, 2020). However, the plain text of the statute is instructive.

The CCPA defines a "business" as a for-profit entity (1) "that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information[;] or" (2) "on the behalf of which that information is collected[;] or" (3) "that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information[.]" Cal. Civ. Code § 1798.140(c) (West 2021). Such an entity must also meet one (1) of the following thresholds to qualify as a "business" under the CCPA: (A) have annual gross revenues in excess of $25 million; (B) annually buy, receive, sell, or share the personal information of 50,000 or more consumers, households, or devices; or (C) earn more than half of its revenue from selling consumers' personal information. *Id.*

***5** Here, California Plaintiffs adequately allege that Blackbaud qualifies as a "business" under the CCPA. First, they specifically maintain that "Blackbaud and its direct customers determine the purposes and means of processing consumers' personal information. Blackbaud uses consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test Blackbaud's services." (ECF No. 77 at 215 ¶ 823.) The CCAC is also filled with claims that Blackbaud develops software solutions to process its customers' patrons' personal information. (*See, e.g.*, *id.* at 7 ¶ 15 ("Blackbaud markets itself to Social Good Entities by developing data-hosting 'solutions' to meet those entities' needs"); 115 ¶ 433 ("Blackbaud determines the purposes or means of processing customers' data based on which solutions or services are utilized by the customers"); 116 ¶ 436 (Blackbaud offers "professional and managed services in which its expert consultants provide data conversion, implementation, and customization services for each of its software solutions").) Second, the California Plaintiffs contend that Blackbaud has "annual gross revenues over $25 million." (*Id.* at 214 ¶ 821.)

Blackbaud's status as a "business" under the CCPA is further supported by Blackbaud's alleged registration as a "data broker" in California. California Plaintiffs claim that Blackbaud is registered as a "data broker" in California pursuant to Cal. Civ. Code § 1798.99.80. (*Id.* at 215 ¶ 824.) Cal. Civ. Code § 1798.99.80 provides that a "data broker" is a "***business*** that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80(d) (West 2021) (emphasis added). The provision also explicitly employs the same definition of "business" as the CCPA, Cal. Civ. Code § 1798.140(c). Cal. Civ. Code § 1798.99.80(a) (West 2021) ("(a) 'Business' has the meaning provided in subdivision (c) of Section 1798.140."). Since an entity must qualify as a "business" under the CCPA in order to be registered as a "data broker" in California, Blackbaud's alleged registration as a "data broker" suggests that it is also a "business" under the CCPA.

Finally, the court rejects Blackbaud's argument that Blackbaud is not a "business" under the CCPA because it qualifies as a "service provider" under the Act. (ECF No. 110-1 at 19.) The CCPA defines "service provider" as

> 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.

Cal. Civ. Code § 1798.140(v) (West 2021). In other words, a "service provider" is a for-profit organization that processes consumer personal information on behalf of a business pursuant to a contract. Thus, a "service provider" could also qualify as a "business" because a "business" is a for-profit organization "that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information[.]" Cal. Civ. Code § 1798.140(c) (West 2021). Accordingly, the statutory definition of "service provider" suggests that "business" is a broader term that encompasses "service provider." Such an interpretation is consistent with the CCPA's direction that the Act "be liberally construed to effectuate its purposes" to "further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information[.]" Cal. Civ. Code §§ 1798.175, 1798.194 (West 2021).

***6** Because Blackbaud could be both a "service provider" and a "business" under the CCPA, it would not be insulated from liability under the CCPA if it qualified as a "service provider." Consequently, the court need not consider whether Blackbaud is a "service provider" under the CCPA to resolve the Motion to Dismiss presently before the court. (ECF No. 110.)

As California Plaintiffs adequately assert that Blackbaud constitutes a "business" under the CCPA, they sufficiently allege violations of the CCPA. Accordingly, the court denies Blackbaud's Motion to Dismiss California Plaintiffs' claims under the CCPA. (*Id.*)

B. California Confidentiality of Medical Information Act Claims

California Plaintiffs also assert claims under California's CMIA. (ECF No. 77 at 214 ¶ 819 – 216 ¶ 833.) The CMIA prohibits a "provider of health care" from disclosing a patient's "medical information" without authorization except in certain specified instances. Cal. Civ. Code § 56.10(a) (West 2021). Blackbaud asserts that California Plaintiffs' CMIA claims should be dismissed because their "medical information" was not exposed as a result of the Ransomware Attack and Blackbaud does not qualify as a "provider of health care" under the CMIA. (ECF No. 110-1 at 23-27.)

California's CMIA applies to "[a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information." Cal. Civ. Code § 56.06(b); *see also* Valerie J. Lopez, *Health Data Privacy: How States Can Fill the Gaps in HIPAA*, 50 U.S.F.L. 313, 326 (2016) (stating "California's CMIA applies to any business that maintains or offers software that maintains medical information.") (citing Cal. Civ. Code § 56.06(b) (West 2013)). The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical

condition, or treatment." Cal. Civ. Code § 56.05(j) (West 2021). Thus, "a prohibited release by a health care provider must include more than individually identifiable information but must also include information relating to medical history, mental or physical condition, or treatment of the individual" to constitute "medical information." *Eisenhower Med. Ctr. v. Superior Court*, 172 Cal. Rptr. 3d 165, 170 (Cal. Ct. App. 2014).

Here, Eisen, Estes, and Regan have not plausibly alleged that "information relating to [their] medical history, mental or physical condition, or treatment" was disclosed during the Ransomware Attack, thus they have failed to sufficiently assert that their "medical information" was exposed as a result of the data breach. *Eisenhower*, 172 Cal. Rptr. 3d at 170. Estes and Regan claim that their names, SSNs, and tax identification numbers were exposed while Eisen maintains that his street addresses and telephone numbers were compromised. (ECF No. 77 at 25 ¶ 63, 27 ¶ 72, 29 ¶ 82.) All assert that it is unknown how much of their PII was exposed during the Ransomware Attack, but none maintain that their PHI could have been compromised. (*Id.* at 25 ¶ 64, 27 ¶ 74, 30 ¶ 84.) It is also not plausible that Eisen's, Estes', and Regan's "medical information" was disclosed during the Ransomware Attack because they allege that their PII was exposed as a result of their relationships with non-profit organizations rather than their interactions with medical providers. Thus, they do not state claims under the CMIA.

***7** However, Clayton plausibly alleges that her "medical information" was disclosed during the Ransomware Attack. She claims Community Medical Centers notified her that her name, address, phone number, email address, date of birth, room number, patient identification number, name of hospital where treated, and applicable hospital department or unit may have been exposed and Trinity Health informed her that her name, address, phone number, email, most recent donation date, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number and physician name were exposed. (ECF No. 77 at 22 ¶ 52.) Furthermore, Clayton contends that "additional medical information, such as [her] diagnosis or treatment plan" may have also been compromised due to Blackbaud's lack of transparency about the scope of the Ransomware Attack. (*Id.* at 22 ¶ 53.) Therefore, the information Clayton alleges was compromised in the Ransomware Attack shows when and where she received medical treatment, which doctors treated her, and whether her treatment required an inpatient stay. If more information was exposed during the Ransomware Attack than initially reported, it may also reveal her medical history, mental and/or physical condition, and specific treatments. Accordingly, Clayton has plausibly alleged that "information relating to [her] medical history, mental or physical condition, or treatment" was exposed during the Ransomware Attack. *Eisenhower*, 172 Cal. Rptr. 3d at 170.

The CMIA's definition of "provider of health care" encompasses traditional medical providers such as nurses, doctors, and hospitals. Cal. Civ. Code § 56.05(m) (West 2021). But in order "to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider[,]" the CMIA's definition of "provider of health care" also includes entities that are not ordinarily considered medical providers, such as technology companies that process and maintain "medical information." *Brown v. Mortensen*, 253 P.3d 522, 533 (Cal. 2011) (explaining the protective purpose of the CMIA); Cal. Civ. Code § 56.06(b) (West 2021) ("Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information ... shall be deemed a provider of healthcare subject to the requirements of this part."). Notably, the CMIA was amended in 2013 to clarify its application to businesses that maintain or offer software that maintains medical information. *See* A.B. 658, chap. 296, 2013 Leg. (Cal. 2013), amending Cal. Civ. § 56.06(b); *see also* Assembly Committee on Appropriations, Bill Analysis, A.B. 658 (May 1, 2013). Specifically, the CMIA defines "provider of health care" in relevant part as

> [a]ny business that offers software or hardware to consumers ... in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or

> management of a medical condition of the individual ....

Cal. Civ. Code § 56.06(b) (West 2021). The purpose of the 2013 amendment of CMIA § 56.06 was to close a loophole "by applying the existing statutory provisions to the newest platform for commercial vendors who offer storage, maintenance, and sharing of sensitive medical information." Lopez, *Health Data Privacy*, *supra*, at 327 (citing Assembly Committee on Appropriations, Bill Analysis, A.B. 658 (May 1, 2013)). Blackbaud falls within this category.

Blackbaud first maintains that it is not a "provider of health care" under Cal. Civ. Code § 56.06(b) because "California Plaintiffs never had direct contact with Blackbaud and at no point purchased a product from Blackbaud." (ECF No. 110-1 at 25.)[4] This argument fails. The statute does not require a business to offer software or hardware directly to a plaintiff in order to qualify as a "provider of health care." In fact, the text of the statute provides that a technology company can be a "provider of health care" even if the "individual" whose information is managed by the technology and the "provider of health care" using the technology are not "consumers" of the technology. *See* Cal. Civ. Code § 56.06(b) (West 2021). Moreover, the statutory language suggests that the definition of "consumers" is not limited to "individuals" because it uses both terms. *See id.* ("[a]ny business that offers software or hardware to ***consumers*** ... in order to make the information available to an ***individual***") (emphasis added).

***8** Second, Blackbaud argues that it cannot be a "provider of health care" because California Plaintiffs fail to allege that Blackbaud collected their information "for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual[.]" (ECF No. 110-1 at 26 (citing Cal. Civ. Code § 56.06(b) (West 2021)).) In amending Cal. Civ. Code § 56.06 to include businesses that maintain or offer software that maintains medical information, the California legislature intended to ensure that the CMIA would apply to all businesses that maintain medical information "whether or not the business was organized for that purpose." Joseph R. Tiffany et al., *The Doctor is in, but your Medical Information is Out*, 24 No. 1 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 206, 225 (2015); *see also* Assembly Committee on Appropriations, Bill Analysis, A.B. 658 (May 1, 2013).

The court observes that Blackbaud's argument requires a tortured reading of the CMIA. Cal. Civ. Code § 56.06(b) does not suggest that a business can only be a "provider of health care" if its software or hardware is used "for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual[.]" Cal. Civ. Code § 56.06(b) (West 2021). Instead, a business can qualify as a "provider of health care" if it offers software or hardware to consumers (1) "in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care," (2) "for purposes of allowing the individual to manage his or her information, or" (3) "for the diagnosis, treatment, or management of a medical condition of the individual[.]" *Id.*

California Plaintiffs plausibly allege that Blackbaud offered its software for such uses. They specifically claim that "Blackbaud's systems were designed, in part, to make medical information available to Social Good Entities by providing cloud-based computing solutions through which those organizations could store, access, and manage consumers' medical information, including but not limited to diagnosing, treating, or managing consumers' medical conditions." (ECF No. 77 at 217 ¶ 840.) Clayton also maintains that she was "required to provide her PHI to several healthcare providers as a predicate to receiving healthcare services" and her "PHI was in turn provided to Blackbaud to be held for safekeeping." (*Id.* at 22 ¶ 52.) Because Clayton claims she provided her PHI to several medical centers in order to receive healthcare services and the medical centers entrusted her PHI to Blackbaud, it is plausible that Blackbaud's software was used "to make the information available to [Clayton] or a provider of health care at the request of [Clayton] or a provider of health care" or "for the diagnosis, treatment, or management of [Clayton's] medical condition[.]" Cal. Civ. Code § 56.06(b) (West 2021). Accordingly, California Plaintiffs plausibly allege that Blackbaud constitutes a "provider of health care" under Cal. Civ. Code § 56.06(b).

In summary, the court grants in part and denies in part Blackbaud's Motion to Dismiss California Plaintiffs' CMIA claims. (ECF No. 110.) The court grants Blackbaud's Motion to Dismiss as to California Plaintiffs Eisen's, Estes', and Regan's CMIA claims because they do not allege that their "medical information" was compromised in the Ransomware Attack. (*Id.*) However, the court denies Blackbaud's Motion to Dismiss as to California Plaintiff Clayton because she sufficiently asserts that her "medical information" was exposed as a result of the Ransomware Attack and that Blackbaud qualifies as a "medical provider" under the CMIA. (*Id.*)

C. Florida Deceptive and Unfair Trade Practice Act Claims

***9** FDUTPA proscribes "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce ...." Fla. Stat. Ann. § 501.204 (West 2021). "To enforce this proscription, the Act has created a private cause of action for damages, Fla. Stat. § 501.211(2), and for declaratory or injunctive relief, Fla. Stat. § 501.211(1)." *Klinger v. Weekly World News, Inc.*, 747 F. Supp. 1477, 1479 (S.D. Fla. 1990). In the present case, Florida Plaintiffs William Carpenella and Dorothy Kamm (collectively, "Florida Plaintiffs") assert FDUTPA claims for damages as well as declaratory and injunctive relief. (ECF No. 77 at 233 ¶ 929 – 237 ¶ 944.)

To state a claim for damages under FDUTPA, a plaintiff must allege: "(1) a deceptive act or unfair practice; (2) causation; and (3) actual damages." *City First Mortgage Corp. v. Barton*, 988 So. 2d 82, 86 (Fla. Dist. Ct. App. 2008). Here, Florida Plaintiffs allege that Blackbaud committed nine (9) deceptive acts or unfair practices. (ECF No. 77 at 234-35 ¶ 933.) In summary, they claim that Blackbaud:

- Failed to adopt reasonable security measures and adequately notify customers and Plaintiffs of the data breach;
- Misrepresented that certain sensitive PII was not exposed during the breach, it would protect Plaintiffs' PII, and it would adopt reasonable security measures; and
- Concealed that it did not adopt reasonable security measures.

(*Id.*) As a result of such alleged deceptive acts or unfair practices, Florida Plaintiffs assert that they suffered damages such as "fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information." (*Id.* at 236 ¶ 943.)

Viewing the CCAC in the light most favorable to Florida Plaintiffs, Florida Plaintiffs have failed to sufficiently establish the "actual damages" leg of the "FDUTPA liability tripod." *Rollins, Inc. v. Butland*, 951 So. 2d 860, 871 (Fla. Dist. Ct. App. 2006). Under FDUTPA, a plaintiff may recover "economic damages related ***solely*** to a product or service purchased in a consumer transaction infected with unfair or deceptive trade practices or acts." *Delgado v. J.W. Courtesy Pontiac GMC-Truck, Inc.*, 693 So. 2d 602, 606 (Fla. Dist. Ct. App. 1997) (emphasis added). A plaintiff may not recover for "damage to property other than the property that is the subject of the consumer transaction." Fla. Stat. Ann. § 501.212(3) (West 2021). Thus, FDUTPA "entitles a consumer to recover damages attributable to the diminished value of the goods or services received, but does not authorize recovery of consequential damages to other property attributable to the consumer's use of such goods or services." *Schauer v. Morse Operations, Inc.*, 5 So. 3d 2, 7 (Fla. Dist. Ct. App. 2009).

In the present case, the data management software Blackbaud provided to Social Good Entities is "the property that is the subject of the consumer transaction." Fla. Stat. Ann. § 501.212(3) (West 2021). Throughout the CCAC, Florida Plaintiffs contend that Social Good Entities purchased software solutions from Blackbaud to store, analyze, and manage their patrons' data. (*See, e.g.*, ECF No. 77 at 6 ¶ 12, 13-14 ¶ 30, 112 ¶ 424, 115 ¶ 431.) They do not maintain that Social Good Entities sold or licensed their patrons' data to Blackbaud. Thus, like the subject of a sale of photo editing software is the software and not the pictures that the purchaser edits with the software, the subject of Social Good Entities' purchase of data management software is the software rather than the data they managed with the software.

Accordingly, Florida Plaintiffs can only recover for damages to the data management products organizations purchased from Blackbaud to maintain Florida Plaintiffs' PII.

***10** However, Florida Plaintiffs allege no such damages. Fraud and identity theft, time and money spent on mitigation, an increased risk of fraud and identity theft, and loss of value of Florida Plaintiffs' PII do not constitute harm to the data management products Social Good Entities purchased from Blackbaud to maintain Florida Plaintiffs' data. (*Id.* at 236 ¶ 943.) Instead, such injuries constitute harm to Florida Plaintiffs' bank accounts, emotional well-being, and data. As Florida Plaintiffs have not alleged damages to "the property that is the subject of the consumer transaction[,]" they have failed to sufficiently assert "actual damages" under FDUTPA. Fla. Stat. Ann. § 501.212(3) (West 2021). Therefore, the court grants Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA claims seeking damages. (ECF No. 110.)

Although Florida Plaintiffs fail to state a claim for damages under FDUTPA, they adequately state a claim for injunctive relief under FDUTPA. FDUTPA makes "declaratory and injunctive relief available to a broader class of plaintiffs than could recover damages." *Smith v. Wm. Wrigley Jr. Co.*, 663 F. Supp. 2d 1336, 1339 (S.D. Fla. 2009). Thus, to state a claim for injunctive relief, "the plain language of the statute requires a plaintiff to allege that the defendant engaged in a deceptive act or practice in trade or commerce, § 501.204(1), and that the plaintiff be a person 'aggrieved' by the deceptive act or practice, § 501.211(1)." *Klinger*, 747 F. Supp. at 1480; *see also Wyndham Vacation Resorts, Inc. v. Timeshares Direct, Inc.*, 123 So. 3d 1149, 1152 (Fla. Dist. Ct. App. 2012).

Blackbaud presently does not dispute that Florida Plaintiffs have alleged that Blackbaud engaged in a deceptive act or unfair practice. (*See* ECF No. 110-1.) Florida Plaintiffs have also plausibly pled that they were "aggrieved" by Blackbaud's allegedly deceptive acts or unfair practices. They maintain that Blackbaud's security failures contributed to the Ransomware Attack that compromised their data, exposing them to fraud and identity theft and diminishing the value of their PII. (ECF No. 77 at 234 ¶ 933 – 236 ¶ 943.) Florida Plaintiffs further assert that Blackbaud's misrepresentations and omissions about its security efforts and the scope of the Ransomware Attack prompted them to take mitigation efforts out of fear that they were at an increased risk for fraud or identity theft. (*Id.*) As Florida Plaintiffs have sufficiently alleged a claim for declaratory and injunctive relief under FDUTPA, the court denies Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA declaratory and injunctive relief claims. (ECF No. 110.)

D. New Jersey Consumer Fraud Act Claims

Blackbaud contends that New Jersey Plaintiffs Martin Roth's and Rachel Roth's (collectively, "New Jersey Plaintiffs") claims under the NJCFA should be dismissed for failure to state a claim. (ECF No. 110-1 at 31-35.) Blackbaud asserts its services do not fall within the purview of the NJCFA because it sells services to sophisticated businesses and entities, not the general public. (ECF No. 110-1 at 32.) As such, New Jersey Plaintiffs are not "consumers" of its services protected by the NJCFA. To state a NJCFA claim, a "consumer" must allege sufficient facts to demonstrate (1) unlawful conduct by the defendant that violates the NJCFA; (2) an ascertainable loss by the plaintiff; and (3) a causal relationship between the unlawful conduct and the ascertainable loss. *Gonzalez v. Wilshire Credit Corp.*, 25 A.3d 1103, 1115 (N.J. 2011) (citing *Lee v. Carter-Reed Co.*, L.L.C., 4 A.3d 561, 576 (N.J. 2010)). "It is well-established that NJCFA claims must meet the heightened pleading requirements of Fed. R. Civ. P. 9(b)." *Lieberson v. Johnson & Johnson Consumer Cos., Inc.*, 865 F. Supp. 2d 529, 538 (D.N.J. 2011) (citing *Frederico v. Home Depot*, 507 F.3d 188, 200 (3d Cir. 2007)). Although Blackbaud does not explicitly contend that New Jersey Plaintiffs lack statutory standing, the court construes Blackbaud's assertion that New Jersey Plaintiffs' claims "fall outside the NJCFA's purview" as a challenge to statutory standing. (ECF No. 110-1 at 31-32, 32 n. 2.)

***11** Statutory standing is a "distinct" concept from Article III and prudential standing. *CGM, LLC v. BellSouth Telecomms., Inc.*, 664 F.3d 46, 52 (4th Cir. 2011). Statutory standing "applies only to legislatively-created causes of action" and concerns "whether a statute creating a private right of action authorizes a particular plaintiff to avail herself of that right of action." *Id.* A motion to dismiss for lack of statutory standing is addressed under Rule 12(b)(6) rather than Rule 12(b)(1) because a "dismissal for lack of statutory

standing is properly viewed as a dismissal for failure to state a claim rather than a dismissal for lack of subject matter jurisdiction." *Id.* (citing *Vaughn v. Bay Envtl. Mgmt., Inc.*, 567 F.3d 1021, 1024 (9th Cir. 2009)).

The NJCFA "provides a private cause of action to consumers who are victimized by fraudulent practices in the marketplace," *Gonzalez*, 25 A.3d at 1114, and prohibits a person from using an "unconscionable commercial practice, deception, fraud," or the like "in connection with the sale or advertisement of any merchandise or real estate." N.J. Stat. Ann. § 56:8-2. Merchandise is defined as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." *Id.* § 56:8- 1. The NJCFA "is not intended to cover every transaction that occurs in the marketplace[,]" instead "[i]ts applicability is limited to consumer transactions which are defined both by the status of the parties and the nature of the transaction itself." *Arc Networks, Inc. v. Gold Phone Card Co.*, 756 A.2d 636, 638 (N.J. Super. Ct. Law Div. 2000) (citing *City Check Cashing, Inc. v. National State Bank*, 582 A.2d 809 (N.J. App. Div. 1990)).

Accordingly, only "consumers" and "commercial competitors" have statutory standing to bring claims under the NJCFA. *800-JR Cigar, Inc. v. GoTo.com, Inc.*, 437 F. Supp. 2d 273, 295-96 (D.N.J. 2006) (citing *Conte Bros. Automotive, Inc. v. Quaker State-Slick 50, Inc.*, 992 F. Supp. 709, 716 (D.N.J. 1998)). In order to recover under the NJCFA as a "consumer," "a Plaintiff must be a consumer of the product *vis-à-vis* the defendant." *In re Managed Care Litig.*, 298 F. Supp. 2d 1259, 1303-04 (S.D. Fla. 2003). Although the NJCFA does not define "consumer," New Jersey courts have interpreted the term to mean "one who uses economic goods and so diminishes or destroys their utilities." *U.S. ex rel. Krahling v. Merck & Co., Inc.*, 44 F. Supp. 3d 581, 607 (E.D. Pa. 2014) (citing *City Check Cashing, Inc. v. Nat'l State Bank*, 582 A.2d 809, 811 (N.J. Super. Ct. App. Div. 1990)).

A plaintiff does not qualify as a "consumer" if they do not purchase a product for consumption. *See Standard Fire Ins. Co. v. MTU Detroit Diesel, Inc.*, No. CIV. A. 07-3827 GEB, 2009 WL 2568199, at *5 (D.N.J. Aug. 13, 2009) (finding that an insurance company asserting an NJCFA claim product defect claim was not a "consumer" because it "did not even purchase the yacht at issue"); *In re Schering-Plough Corp. Intron/Temodar Consumer Class Action*, No. 2:06-CV-5774(SRC), 2009 WL 2043604, at *31 (D.N.J. July 10, 2009) ("Products and services that are purchased for consumption or use in the operation of a business are covered by the NJCFA.") (concluding that third-payor payers who did not "use or consume the drugs they purchase[d]" were not "consumers" of the drugs they purchased); *Windsor Card Shops, Inc. v. Hallmark Cards, Inc.*, 957 F. Supp. 562, 567 n.6 (D.N.J. 1997) (holding that a corporation "cannot sue as a consumer of goods under [the] NJCFA" when it "purchased the goods at wholesale to sell to its store customers").

***12** Here, New Jersey Plaintiffs are not "consumers" entitled to the protection of the NJCFA. Martin Roth alleges that Blackbaud maintained his data as a result of his relationship with Joseph Kushner Hebrew Academy and claims that the school retained his data because his "children attended Joseph Kushner Hebrew Academy and he also made charitable donations during the time his children attended the school." (ECF No. 77 at 66 ¶ 231.) Such assertions do not plausibly establish that Martin Roth was a "consumer" of Blackbaud's data management services. They do not suggest that Martin Roth knew that Blackbaud existed or managed his data on behalf of Joseph Kushner Hebrew Academy, let alone that he purchased and used Blackbaud's services. Further, Martin Roth's donation to Joseph Hebrew Academy does not render him a "consumer" of philanthropy. Donors are not "consumers" under the NJCFA because they are "not being approached in their commonly accepted capacity as consumers" and a donation "involves neither commercial goods nor commercial services." *See Del Tufo v. Nat'l Republican Senatorial Comm.*, 591 A.2d 1040, 1042 (N.J. Super. Ct. Ch. Div. 1991). Thus, the CCAC does not plausibly allege that Martin Roth purchased any services for consumption.

Similarly, Rachel Roth does not plausibly contend that she is a "consumer" of Blackbaud's services. Rachel Roth claims that Blackbaud stored her data as a result of her attendance at Joseph Kushner Hebrew Academy from 2005 through 2014. (ECF No. 77 at 68 ¶¶ 239, 240.) But like

Martin Roth, she does not assert that she purchased or used Blackbaud's services, knew Blackbaud existed, or perceived that Blackbaud managed her data. (*See id.* at 67 ¶ 238 – 69 ¶ 246.)

Therefore, New Jersey Plaintiffs fail to state claims under the NJCFA because they do not plausibly allege that they are "consumers" of services entitled to the NJCFA's protection. Accordingly, the court grants Blackbaud's Motion to Dismiss New Jersey Plaintiffs' NJCFA claims. (ECF No. 110.)

E. New York General Business Law § 349 Claims

New York Plaintiffs Ralph Peragine and Karen Zielinski (collectively, "New York Plaintiffs") assert claims under GBL § 349. (ECF No. 77 at 342 ¶ 1443 – 344 ¶ 1451.) To bring a claim for a violation of GBL § 349, a plaintiff must plausibly allege three elements: (1) "the challenged act or practice was consumer-oriented;" (2) the act or practice "was misleading in a material way;" and (3) "the plaintiff suffered injury as a result of the deceptive act[.]" *Stutman v. Chem. Bank*, 731 N.E.2d 608, 611 (N.Y. 2000). Blackbaud contends that New York Plaintiffs have failed to establish the first element of a GBL § 349 claim.

An act or practice is "consumer-oriented" if it has "a broader impact on consumers at large." *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 647 N.E.2d 741, 744 (N.Y. 1995). Thus, "[p]laintiffs must allege conduct that implicates the public interest, something more than a single-shot consumer transaction or a contract dispute unique to the parties." *Phifer v. Home Savers Consulting Corp.*, No. 06 CV 3841 (JG), 2007 WL 295605, at *5 (E.D.N.Y. Jan. 30, 2007) (citing *Teller v. Bill Hayes, Ltd.*, 630 N.Y.S.2d 769 (N.Y. App. Div. 1995)). However, GBL § 349 does "not impose a requirement that consumer-oriented conduct be directed to all members of the public[.]" *Plavin v. Grp. Health Inc.*, 146 N.E.3d 1164, 1170 (N.Y. 2020). The "consumer-oriented" act or practice requirement has been "construed liberally." *New York v. Feldman*, 210 F. Supp. 2d 294, 301 (S.D.N.Y. 2002).

Contrary to Blackbaud's assertions, New York Plaintiffs adequately plead that Blackbaud's allegedly deceptive acts were "consumer-oriented." New York Plaintiffs allege that Blackbaud engaged in nine (9) deceptive acts or practices in violation of GBL § 349. (ECF No. 77 at 342-43 ¶ 1444.) Essentially, they assert that Blackbaud:

- Failed to implement reasonable security measures and timely and adequately notify Blackbaud customers, New York Plaintiffs, and New York Subclass members of the data breach;
- Misrepresented its security measures and the scope of the data breach; and

***13** • Concealed the fact that it did not reasonably secure the PII and/or PHI of New York Plaintiffs and New York Subclass members.

(*Id.*)

Viewing the CCAC in the light most favorable to New York Plaintiffs, New York Plaintiffs plausibly claim that such deceptive acts had "a broader impact on consumers at large." *Oswego*, 647 N.E.2d at 744. They maintain that Blackbaud's misrepresentations and omissions deceived donors, patients, students, and congregants in New York to believe they did not need to take actions to secure their identities because their data was not exposed. (ECF No. 77 at 6 ¶ 11, 343-44 ¶ 1446.) They also assert that Blackbaud's deceptions misled donors, patients, students, and congregants in New York about the adequacy of Blackbaud's data security. (*Id.* at 6 ¶ 11, 343 ¶ 1445.) Specifically, New York Plaintiffs claim that they would not have entrusted their PII and/or PHI to a Social Good Entity if they had known that one of the primary cloud computing vendors the entity entrusted with their PII and/or PHI failed to maintain adequate data security. (*Id.* at 69-70 ¶ 248, 72 ¶ 258.) Such allegations suggest that Blackbaud's allegedly deceptive acts caused donors, patients, students, and congregants in New York to suffer avoidable injuries such as identity theft and diminished data value. Accordingly, it is plausible that Blackbaud's misrepresentations and omissions impacted a broad segment of New York consumers.

As privity is not required to state a claim under GBL § 349, it is irrelevant that New York Plaintiffs are not direct consumers of Blackbaud. *See* *Bildstein v. MasterCard Int'l*, Inc., No. 03 CIV.9826I(WHP), 2005 WL 1324972, at *3 (S.D.N.Y. June 6, 2005).

> While the typical case under section 349 generally involves claims arising directly out of a commercial transaction between a plaintiff consumer and a defendant seller, neither the text of the statute nor the case law establishes this requirement. The phrase "commercial transaction" can be found nowhere in the plain language of the statute, and section 349(h) specifically empowers "[a]ny person who has been injured by reason of any violation of this section" to bring an action. GBL § 349(h). Indeed, "[t]here is no requirement of privity, and victims of indirect injuries are permitted to sue under the Act."

In re Methyl Tertiary Butyl Ether Products Liab. Litig., 175 F. Supp. 2d 593, 630-31 (S.D.N.Y. 2001) (quoting *Vitolo v. Dow*, 634 N.Y.S.2d 362 (N.Y. Sup. Ct. 1995)). "The critical question, then, is whether the matter affects the public interest in New York, not whether the suit is brought by a consumer or a competitor." *Securitron Magnalock Corp. v. Schnabolk*, 65 F.3d 256, 264 (2d Cir. 1995).

Furthermore, Blackbaud's allegedly deceptive acts are similar to other acts that courts have found to be "consumer-oriented" under GBL § 349. Conduct has been held to be sufficiently consumer-oriented to satisfy the statute "where it involved 'an extensive marketing scheme,' where it involved the 'multi-media dissemination of information to the public,' and where it constituted a standard or routine practice that was 'consumer-oriented in the sense that [it] potentially affect[ed] similarly situated consumers.' " *Tomassini v. FCA U.S. LLC*, No. 3:14-CV-1226 MAD/DEP, 2015 WL 3868343, at *4 (N.D.N.Y. June 23, 2015) (quoting *N. State Autobahn, Inc. v. Progressive Ins. Grp. Co.*, 953 N.Y.S.2d 96, 102 (N.Y. App. Div. 2012)). Additionally, "courts have allowed claims under Section 349 where misleading statements are made to third parties resulting in harm to consumers." *Bose v. Interclick, Inc.*, No. 10 CIV. 9183 DAB, 2011 WL 4343517, at *8 (S.D.N.Y. Aug. 17, 2011) (citing *Securitron*, 65 F.3d at 264; *Kuklachev v. Gelfman*, 600 F. Supp. 2d 437, 476 (E.D.N.Y. 2009)).

***14** In the present case, New York Plaintiffs assert that Blackbaud's public misrepresentations about the scope of the Ransomware Attack misled Plaintiffs into believing they did not need to take mitigation measures against identity theft and fraud. (ECF No. 77 at 343-44 ¶ 1446.) Such conduct is akin to an "extensive marketing scheme" utilizing "multi-media dissemination of information to the public" since Blackbaud allegedly promulgated misrepresentations about the extent of the Ransomware Attack through media interviews, its website, and Social Good Entities. (*Id.* at 9 ¶ 20, 16 ¶ 36, 70 ¶ 251, 72-73 ¶ 261, 138 ¶ 499.) New York Plaintiffs also claim that "misleading statements [were] made to third parties resulting in harm to consumers" because they contend Blackbaud's misrepresentations about its data security to its customers prevented consumers from protecting their data. (*Id.* at 6 ¶ 11, 69-70 ¶ 248, 72 ¶ 258, 343 ¶ 1445.)

Since New York Plaintiffs have sufficiently alleged that Blackbaud engaged in acts in violation of GBL § 349 that were "consumer-oriented," the court denies Blackbaud's Motion to Dismiss New York Plaintiffs' GBL § 349 claims. (ECF No. 110.)

F. Pennsylvania Unfair Trade Practices and Consumer Protection Law Claim

Pennsylvania Plaintiff Christina Duranko ("Pennsylvania Plaintiff") asserts a claim under the UTPCPL. (ECF No. 77 at 362 ¶ 1531 – 365 ¶ 1542.) The UTPCPL provides a private cause of action to "[a]ny person who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by any person of a method, act or practice declared unlawful" by the Act. 3 Pa. Stat. Ann. § 201-9.2 (West 2021). To maintain a private right of action under the UTPCPL, "a plaintiff must show that he justifiably relied on the defendant's wrongful conduct or representation and that he suffered harm as a result of that reliance." *Yocca v. Pittsburgh Steelers Sports, Inc.*, 854 A.2d 425, 438 (Pa.

2004); *see also* *Hunt v. U.S. Tobacco Co.*, 538 F.3d 217, 221 (3d Cir. 2008). "It is the plaintiff's burden to prove justifiable reliance in the complaint." *Riviello v. Chase Bank USA, N.A.*, No. 3:19-CV-0510, 2020 WL 1129956, at *4 (M.D. Pa. Mar. 4, 2020) (citing *Weinberg v. Sun Co., Inc.*, 777 A.2d 442, 446 (Pa. 2001)). Pennsylvania Plaintiff has failed to meet this burden.

Pennsylvania Plaintiff's UTPCPL claim is premised on both Blackbaud's alleged misrepresentations and its alleged omissions. She asserts that Blackbaud misrepresented that it would protect the privacy and confidentiality of her information, the scope of the Ransomware Attack, and that it would comply with common law and statutory duties pertaining to the security and privacy of her information. (ECF No. 77 at 362-63 ¶ 1535). She also maintains that Blackbaud omitted that it did not adequately secure her information or comply with common law and statutory duties pertaining to the security and privacy of her information. (*Id.*)

However, Pennsylvania Plaintiff does not sufficiently allege that she relied on such alleged misrepresentations and omissions. She claims that she was "required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services[,]" her PHI "was in turn provided to Blackbaud to be held for safekeeping[,]" and she suffered injuries as a result of her "reliance" on Blackbaud's misrepresentations and omissions. (*Id.* at 85 ¶ 310, 364 ¶ 1541.) But the CCAC is bereft of allegations suggesting that Pennsylvania Plaintiff knew that Blackbaud maintained her data or was exposed to representations Blackbaud made to her or her healthcare provider. In fact, the CCAC does not even assert that Pennsylvania Plaintiff knew that Blackbaud existed. Pennsylvania Plaintiff does maintain that she "would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security." (*Id.* at 84-85 ¶ 309.) However, such an assertion is nothing more than a conclusory allegation. Thus, even viewing the CCAC in the light most favorable to Pennsylvania Plaintiff, Pennsylvania Plaintiff has failed to adequately establish the reliance requirement of a UTPCPL claim.

***15** Recognizing the weakness of her claim, Pennsylvania Plaintiff asks the court to "hold that [her] UTPCPL theories based on Blackbaud's omissions may nonetheless proceed" because reliance is not an element of an omission-based UTPCPL claim. (ECF Nos. 123 at 38 n.11; 137 at 58:13-17.) Such an interpretation of UTPCPL case law "relaxes the 'justifiable reliance' element of a UTPCPL claim far too much[.]" *In re Rutter's Inc. Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 29054, at *20 (M.D. Pa. Jan. 5, 2021). Pennsylvania courts "have presumed reliance [in UTPCPL cases] only under narrow circumstances not present here, such as securities fraud[ ] and manufacturing defects[.]" *Moore v. Angie's List, Inc.*, 118 F. Supp. 3d 802, 817 n.8 (E.D. Pa. 2015).

Pennsylvania Plaintiff correctly notes that plaintiffs were not required to establish reliance to prove their omission-based UTPCPL claims in *Drayton v. Pilgrim's Pride Corp.*, No. 03-2334, 2004 WL 765123 (E.D. Pa. Mar. 31, 2004) and *Zwiercan v. Gen. Motors Corp.*, 58 Pa. D. & C. 4th 251 (Pa. Com. Pl. 2002). (ECF No. 123 at 37.) However, *Drayton* and *Zwiercan* stand for the limited proposition that reliance can be presumed in UTPCPL actions where a manufacturer knows of a dangerous safety defect that customers would be unable to discover themselves. *Drayton*, 2004 WL 765123, at *7 (citing *Zwiercan*, 58 Pa. D. & C. 4th 251). *Drayton* presumed the reliance element of a UTPCPL claim against defendant poultry processing plants by a plaintiff whose husband died from ingestion of listeria-contaminated meat, while *Zwiercan* did not require a plaintiff car purchaser to establish the reliance element in a UTPCPL action against a defendant car manufacturer for dangerously defective front seats. 2004 WL 765123, at *7; 58 Pa. D. & C. 4th 251. In other words, *Drayton* and *Zwiercan* both involved manufacturers of potentially-dangerous products that "allegedly knew their product was adulterated and therefore dangerous, and would therefore have a duty to advise unsophisticated consumers of that material fact." *Drayton*, 2004 WL 765123, at *7 (citing *Zwiercan*, 58 Pa. D. & C. 4th 251). Acknowledging that the decision to presume reliance in both cases was driven by the life-threatening consequences of the omissions at issue, the court in *Drayton* explicitly noted that "in normal UTPCPL false advertising claims reliance is required[.]" *Id.*

The facts of the present case are more similar to a "normal UTPCPL false advertising claim[ ]" than to the facts in *Drayton* and *Zwiercan*. *Id.* Defendants in data breach cases cannot be "aptly compared to a car manufacturer or a meat-processing plant" because they are "not duty-bound, like a car manufacturer with front seat defects or meat-processer with a listeria outbreak, to alert customers or state or federal officials as to any potential data-security issues." *In re Rutter's*, 2021 WL 29054, at *21. Here, Pennsylvania Plaintiff did not purchase a potentially-dangerous product that would impose a duty on Blackbaud to notify Pennsylvania Plaintiff or government officials of any potential data-security issues. Unlike the omissions in *Drayton* and *Zwiercan*, Blackbaud's alleged omissions about its data security practices did not expose its customers and their patrons to life-or-death consequences.

Pennsylvania Plaintiff's UTPCPL data breach claim also differs from the UTPCPL product defect claims at issue in *Drayton* and *Zwiercan* because "the plaintiffs in *Zwiercan* and *Drayton* were totally unable to establish the reliance element—in both cases, 'the unsophisticated Plaintiff is at the mercy of the Defendant to inform her of a known safety defect.' " *Id.* at *21 (quoting *Zwiercan*, 58 Pa. D. & C. 4th 251). In contrast, Blackbaud made representations about its security infrastructure and the scope of the Ransomware Attack in the present case. Pennsylvania Plaintiff does not assert that she relied on such representations when deciding to entrust her data to her healthcare provider and Blackbaud. Given that this case does not involve a potentially-dangerous product and Pennsylvania Plaintiff could have established the reliance element of a UTPCPL claim based on Blackbaud's alleged misrepresentations, the court finds that the reliance presumption enunciated in *Drayton* and *Zwiercan* does not apply here. This conclusion is supported by the United States District Court for the Middle District of Pennsylvania's decision not to extend the reliance presumption articulated in *Drayton* and *Zwiercan* to the data breach context in *In re Rutter's*. 2021 WL 29054, at *21.

***16** As Pennsylvania Plaintiff does not sufficiently assert that she justifiably relied on Blackbaud's alleged misrepresentations and omissions and a presumption of reliance does not apply to the facts of this case, Pennsylvania Plaintiff has failed to establish the justifiable reliance requirement of a UTPCPL claim. Accordingly, the court grants Blackbaud's Motion to Dismiss Pennsylvania Plaintiff's UTPCPL claim. (ECF No. 110.)

G. South Carolina Data Breach Security Act Claims

South Carolina Plaintiffs Latricia Ford and Clifford Scott (collectively, "South Carolina Plaintiffs") advance SCDBA claims under S.C. Code Ann. § 39-l-90(a). (ECF No. 77 at 370 ¶ 1574 – 372 ¶ 1581.) S.C. Code Ann. § 39-l-90(A) requires a person conducting business in South Carolina and "***owning or licensing*** computerized data or other data that includes personal identifying information" to notify South Carolina residents in the event of a data breach. S.C. Code Ann. § 39-1-90(A) (West 2021) (emphasis added). Blackbaud maintains that it is not liable under the SCDBA because it does not "own[ ] or licens[e]" data. (ECF No. 110-1 at 41-44 (citing S.C. Code Ann. § 39-l-90(A) (West 2021)).) The court agrees.

The CCAC features the conclusory assertion that Blackbaud "is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A)." (ECF No. 77 at 371 at ¶ 1575.) However, it does not "contain sufficient factual matter" to plausibly allege that Blackbaud "own[s] or licens[es]" data. *Iqbal*, 556 U.S. at 678; S.C. Code Ann. § 39-l-90(A) (West 2021). The CCAC suggests that Blackbaud possesses data, contending that Social Good Entities "entrusted Plaintiffs' and class members' data to Blackbaud" and Blackbaud "hosted" information from Social Good Entities. (ECF No. 77 at 7-8 ¶ 15, 8 ¶ 16, 11 ¶ 24.) But it does not assert that Blackbaud has an ownership interest or other form of legal entitlement to the data it receives from Social Good Entities and their patrons. Possession may be a necessary condition of "owning or licensing[,]" but it is not sufficient to establish "owning or licensing[.]" S.C. Code Ann. § 39-l-90(A) (West 2021). In fact, South Carolina Plaintiffs' counsel admitted at the hearing that they "alleged the bare minimum in [their] complaint" and professed "it's really difficult to stand here and argue that [Blackbaud is] without a doubt an owner or licensor without additional information." (ECF No. 137 at 60:1-3.) "Labels, conclusions, recitation of a claim's elements, and naked assertions devoid of further factual enhancement will not suffice to meet the Rule 8 pleading standard." *ACA Fin. Guar. Corp. v. City of Buena Vista, Virginia*, 917 F.3d 206, 211 (4th Cir. 2019). As the CCAC contains nothing

more than a naked assertion that Blackbaud "is a business that owns or licenses" data, South Carolina Plaintiffs have failed to plausibly allege that Blackbaud is a business "owning or licensing" data under S.C. Code Ann. § 39-l-90(A). (ECF No. 77 at 371 at ¶ 1575); S.C. Code Ann. § 39-l-90(A) (West 2021).

In their Response, South Carolina Plaintiffs assert that they state a claim under the SCDBA because they fulfill the pleading requirements for a SCDBA claim under S.C. Code Ann. § 39-l-90(B). (ECF No. 123 at 39-41.) This argument is unavailing. Unlike S.C. Code Ann. § 39-l-90(A) which only applies to those "***owning or licensing***" data, S.C. Code Ann. § 39-l-90(B) requires a person doing business in South Carolina and "***maintaining*** computerized data or other data that includes personal identifying information that the person does not own" to notify the owner or licensee of the information after a data breach. S.C. Code Ann. § 39-l-90(A)-(B) (West 2021) (emphasis added). Thus, S.C. Code Ann. § 39-l-90(A) and S.C. Code Ann. § 39-l-90(B) provide for separate claims. *See Morgan v. Haley*, No. 2012-CP-4007331, 2013 WL 8335566, at *2 (S.C. Com. Pl. February 27, 2013) (noting that the plaintiff asserted "two separate claims" under S.C. Code Ann. § 39-l-90(A) and S.C. Code Ann. § 39-l-90(B)). Here, South Carolina Plaintiffs explicitly pursue claims under S.C. Code Ann. § 39-l-90(A) and fail to even reference S.C. Code Ann. § 39-l-90(B) in the CCAC. (ECF No. 77 at 370 ¶ 1574 – 372 ¶ 1581.) Since they fail to provide "a short and plain statement of [a S.C. Code Ann. § 39-l-90(B)] claim showing that [they are] entitled to relief[,] South Carolina Plaintiffs do not assert claims under S.C. Code Ann. § 39-l-90(B) in the CCAC. Fed. R. Civ. P. 8(a)(2).

***17** As South Carolina Plaintiffs only assert a SCDBA claim under S.C. Code Ann. § 39-l-90(A) and do not plausibly allege that Blackbaud is a business "owning or licensing" data, the court grants Blackbaud's Motion to Dismiss South Carolina Plaintiffs' SCDBA claims. (ECF No. 110.)

IV. CONCLUSION

For the foregoing reasons, the court **GRANTS IN PART** and **DENIES IN PART** Blackbaud's Motion to Dismiss. (ECF No. 110.) Specifically, the court:

- Denies Blackbaud's Motion to Dismiss California Plaintiffs' CCPA claims;
- Grants Blackbaud's Motion to Dismiss California Plaintiffs Eisen's, Estes', and Regan's CMIA claims;
- Denies Blackbaud's Motion to Dismiss California Plaintiff Clayton's CMIA claim;
- Grants Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA claims seeking damages;
- Denies Blackbaud's Motion to Dismiss Florida Plaintiffs' FDUTPA declaratory and injunctive relief claims;
- Grants Blackbaud's Motion to Dismiss New Jersey Plaintiffs' NJCFA claims;
- Denies Blackbaud's Motion to Dismiss New York Plaintiffs' GBL § 349 claims;
- Grants Blackbaud's Motion to Dismiss Pennsylvania Plaintiff's UTPCPL claim; and
- Grants Blackbaud's Motion to Dismiss South Carolina Plaintiffs' SCDBA claims.

IT IS SO ORDERED.

All Citations

Slip Copy, 2021 WL 3568394

Footnotes

1 As of August 12, 2021, this MDL is comprised of twenty-nine (29) member cases.

2 All named Plaintiffs are identified in paragraphs forty-five (45) through 418 of the CCAC. (*See* ECF No. 77 at 20 ¶ 45 – 110 ¶ 418.)

3 The CCAC supersedes all other complaints in this MDL filed on behalf of Blackbaud's customer's patrons against Blackbaud. (ECF Nos. 23 at 4; 77.) Although the docket reflects that the CCAC was not publicly filed until April 16, 2021, Plaintiffs provided Blackbaud and the court with the CCAC on April 2, 2021 to facilitate the sealing process and maintain the cadence of this litigation. (ECF Nos. 66; 72; 76; 77.)

4 As there is presently no case law interpreting Cal. Civ. Code § 56.06(b), the court will rely on the text of the statute and legislative history to resolve Blackbaud's challenge.