ARTICLE

Reconciling Competing Data Security Standards Applicable to Data Held by Retail Banks Operating in California in Light of *Van Buren* and *TransUnion*

Michael R. Sneberger*

When operating in California, retail banks face competing, seemingly inconsistent, federal, state, and industry data security standards. The article describes what regulations prescribe data security standards for banks operating in California. It analyses private rights of action available in the event of a data breach, how such private rights may be affected by the Van Buren and TransUnion decisions, and what data security standards are set forth by each of the controlling regulatory regimes, as well as other industry standards which may inform the applicable standard of care regarding non-personal information. Finally, the article presents a position on how a California bank can reconcile the applicable security standards, and provides a suggestion for a data security benchmark for retail banks operating in California by positing that a 'reasonable' data security program is not only one based on assessment of risk and industry best practices, but is also reconcilable with the seemingly competing regulatory regimes applicable to banks operating in California.

Keywords: California, Data Security, Security Standards, Retail Banks, Van Buren, TransUnion

1 Introduction

When operating in California, retail banks face competing, seemingly inconsistent, federal, state, and industry data security standards. Section two describes what regulations prescribe data security standards for banks operating in California. Section three analyses private rights of action available in the event of a data breach, how such a private rights may be affected by the *Van Buren*[1] and *TransUnion*[2] decisions, and what data security standards are set forth by each of the controlling regulatory regimes, as well as other industry standards which may inform the applicable standard of care regarding non-personal information. Section four presents a position on how a California bank can reconcile the applicable security standards, and provides a suggestion for a data security benchmark for retail banks operating in California by positing that a 'reasonable' data security program is not only one based on assessment of risk and industry best practices, but is also reconcilable with the seemingly competing regulatory regimes applicable to banks operating in California.

2 Regulatory regimes applicable to banks operating in California that set forth data security requirements

Banks are subject to a myriad of laws, regulations, and rules at the international, federal, and state levels.[3] This article will narrow its focus to the data security standards that are established by the Gramm-Leach-Bliley Act (GLBA)[4] and by the private right of action set forth in the California Consumer Privacy Act (CCPA) as amended

Notes

* Graduate of the University of Minnesota Law School. Licensed to practice in Arizona and Minnesota. He has obtained Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Manager (CIPM) certifications from the International Association of Privacy Professionals and is currently master's degree candidate in Computer Science at Arizona State University's Ira A. Fulton College of Engineering in the School of Computing and Augmented Intelligence. Special thank you to attorney Matthew D. Williams for proofreading and solid advice. The genesis of this article was a paper written for Professors Gary E. Marchant and Guy A. Cardineau's LAW 703 Law, Science, and Technology class in the Fall of 2020 at the Arizona State University Sandra Day O'Connor College of Law. Email: msneberger@cox.net.

1 *Van Buren v. United States*, 593 US ___ (2021) (no. 19-783. Argued 30 Nov. 2020 – Decided 3 June 2021).

2 *TransUnion v. Ramirez*, 594 US ___ (2021) (no. 20-297. Argued 30 Mar. 2021 – Decided 25 June 2021).

3 This article is limited to chartered banks which serve individuals in order to avoid analysis of on-the-margin, non-bank financial services organizations such as automobile dealers who carry notes or lease cars. However, the analysis set forth herein is generally applicable to all financial service organizations handling personal information. *See generally* 15 U.S.C. § 6809(3)(A) ('In general the term "financial institution" means any institution the business of which is engaging in financial activities as described in s. 1843 or title 12'). Similarly, this article limits itself to federally and California chartered banks that are operating in California and not subject to state laws other than those of the State of California in addition to the federal bank regulatory regime. Banks operating under state charters other than California or operating in states where state laws or regulations provide not inconsistent, greater protection than the federal regulatory regime will need to review any state-level data security regulations in addition to those discussed herein. *See e.g.*, *infra* n. 21.

4 The GLB Financial Modernization Act 15 U.S.C. §§ 6801–6827 (1999).

by the recently passed California Privacy Rights Act (CPRA).[5] It will also discuss other, ancillary data security standards. All banks are subject to GLBA which preempts state law to the extent state laws do not afford greater protection than that set forth in GLBA,[6] and banks of sufficient size that serve residents of California are also subject to CCPA.[7] The difficulty for bank compliance and security functions is that these two regulatory regimes offer different presentations of data security regulation.[8]

2.1 *GLBA Preemption of CCPA*

While GLBA generally regulates financial institutions, and CCPA regulates data privacy generally, they each provide a data security requirement. At first glance, GLBA and CCPA do not clash as CCPA specifically exempts 'personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations … ',[9] and GLBA provides that it:

> shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.

It further provides[10]:

> a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter.

GLBA preempts CCPA only to the extent that CCPA does not afford California residents greater protection than GLBA.

Building upon the preemption exclusion language of GLBA which allows state statues 'afford[ing] … greater protection', CCPA excludes from its own exemption of personal information collected pursuant to GLBA its section 1798.150 which in turn provides that:

> [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 for ... statutory damages of between one hundred and seven hundred and fifty dollars per consumer per incident or actual damages, injunctive or declaratory relief, or other relief deemed proper by court 'if prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provision of this title the consumer alleges have been or are being violated'.[11]

Notes

[5] Cal. Civ. Code §§ 1798.100–1798.199 (CCPA); on 3 Nov. 2020 the California electorate approved 'Proposition 24' also known as CPRA which provides for both a comprehensive amendment of CCPA, and the creation of a new, independent enforcement agency called the California Privacy Protection Agency with an effective date of 1 Jan. 2023 and a look-back period to 1 Jan. 2020 so as to match the effective date of CCPA. At the time of the writing of this article the regulations associated with the newly enacted CPRA have been neither promulgated nor adopted. However, the text of CPRA is explicit and its effect on data security standards will be addressed throughout.

[6] 15 U.S.C. § 6807.

[7] CCPA defines a covered 'business' as having 'annual gross revenues in excess of twenty-five million dollars' or as annually sharing for commercial purposes 'the personal information of fifty thousand or more consumers, households, or devices'. Cal. Civ. Code § 1798.140(c)(A)-(B). While CPRA has retained the overall alternative qualification structure of Cal. Civ. Code § 1798.140(c) it has amended para. (A) to slightly enlarge the revenue definition to catch business that 'had' as of the first day of the calendar year twenty-five million dollars in annual gross revenue even if the revenue declines throughout the year but goes multiple directions with para. (B)'s alternative qualification, raising CCPA's fifty thousand threshold, while simultaneously removing devices from the dragnet and also eliminating that the sale or sharing of data needs to be for 'commercial purposes' in order to qualify. The amended language is as follows: '(B) Alone or in combination, annually buys or~~, receives for the business's commercial purposes,~~ sells or shares ~~for commercial purposes, alone or in combination~~ the personal information of ~~50,000~~ 100,000 or more consumers or~~,~~ households~~, or devices~~'.

[8] *See infra* s. 3.

[9] Cal. Civ. Code § 1798.145(e).

[10] 15 U.S.C. § 6807(a)-(b).

[11] Cal. Civ. Code § 1798.150(a)(1) (referring to Cal. Civ. Code § 1798.81.5 which provides a definition of 'personal information'.); CPRA has amended CCPA's private right of action to not only cover nonredacted and nonencrypted personal information but also to include the unauthorized access to a consumer's 'email address in combination with a password or security question and answer that would permit access to the [consumer's] account' thus correcting what appears to have been a drafting oversight by matching CCPA/CPRA's loss of personal information to the definition of personal information found in Cal. Civ. Code § 1798.81.5(d)(1)(B).
Cal. Civ. Code § 1798.150(b) provides that prior to filing an action under para. (a) of the s. for statutory damages (but not for actual pecuniary damages), a plaintiff must first provide a potential defendant '[thirty] days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated', and further provides that if a cure is possible and the potential defendant 'provides the consumer an express written statement what the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated'. CPRA has made a significant change to this notice provision by adding the sentence '[t]he implementation and maintenance of reasonable security procedures and practices pursuant to s. 1798.81.5 following a breach does not constitute a cure with respect to that breach'. CPRA § 1798.150(b). It is not clear what an express written statement of cure under CCPA must contain, and one can anticipate private rights of action continuing after the provision of such an express statement of cure based on plaintiffs' allegation that defendant did not in fact cure, and if the express written statement of cure contains a detailed list of actions that were taken to effect the cure it could become a roadmap to plaintiffs' discovery program. Comments of Mark David McPherson, partner at Morrison & Foerster, during the webinar 'CCPA Litigation and Enforcement Trends: Best Practices for Your Company' held 3 Nov. 2020, https://www.mofo.com/resources/events/201103-ccpa-litigation-enforcement.html(accessed 19 July 2021).

Because there is no private right of action provided in GLBA,[12] the private right of action provided by CCPA presumably 'affords … greater protection' than GLBA and is therefore not preempted.

2.2 *Only Individuals Are Protected by Data Security Standards Mandated by CCPA and GLBA*

Additionally, there exists personal information gathered from consumers of retail banks in California that is not subject to the preemption of GLBA because GLBA defines a 'consumer' – who does not gain privacy rights under the Act – as an individual.[13] Specifically, GLBA defines a 'Customer' – who does gain privacy rights under the Act – as 'a consumer who has a "customer relationship" with a financial institution', and a customer relationship is defined as a continuing relationship established when a consumer maintains a deposit or investment account; obtains a loan; enters into a lease of personal property; or obtains investment advisory services for a fee from the regulated institution. Under GLBA, all Customers who gain rights under the statute are consumers, but not all consumers are Customers, and both are individuals.[14]

Turning to CCPA, a 'consumer' is defined as 'natural person' who is a California resident.[15] This article will refer to a consumer who has established a customer relationship with a bank and thereby become subject to the protections set forth in GLBA as a Customer, while a consumer who has not obtained Customer status will be referred to as a consumer or customer. This means that the data security regulations applicable by way of GLBA and CCPA only apply to the data, specifically the personal information,[16] that a bank holds relating to an individual, more specifically to any individual under CCPA, and only individuals with a customer relationship under GLBA.

2.3 *'Zombie Data' not Covered by Any Security Standard Mandated by Law*

Because CCPA and GLBA only address the data security of the data a bank operating in California holds related to individuals, there is a category of data held by a bank, whose security is not governed by either federal or state statutes or regulations. Such data which is subject to the data security regulations of neither GLBA nor CCPA will be referred to as 'Zombie Data'. For example, data a bank obtained from commercial customers or family trust customers is Zombie Data because it is related to non-individual customers.[17]

Notes

[12] *See infra* n. 75.

[13] 15 U.S.C. § 6809(9).

[14] The road to the definition of 'Customer' under GLBA is winding: '[i]t is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its *{C}ustomers* and to protect the security and confidentiality of those [*C*]*ustomers*' nonpublic person information'. 15 U.S.C. § 6801(a) (emphasis added). This means GLBA extends its security protections to Customers rather than consumers. What is the difference? 'The term "consumer" means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual'. 15 U.S.C. § 6809(9) (the statute itself does not define Customer even though it uses the term extensively). To take a further step in the relationship, the regulations associated with the Financial Privacy Rule of GLBA states that a 'Customer means a consumer who has a customer relationship with' the institution. 16 C.F.R. § 313.3(h), *see also* 12 C.F.R. § 1016.3(i) (Regulation P). Regulations regarding GLBA's 'Safeguards Rule' are found in 16 C.F.R. § 314 which indicates that 'the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 C.F.R. part 313'. *Ibid.*, § 314.2(a). Finally, a 'Customer relationship means a continuing relationship between consumer and [institution] under which [the institution] provide[s] one of more financial products or services to the consumer that are to be used primarily for personal, family or household purposes'. 16 C.F.R. § 313.3(i)(1), *see also* (i)(2)(i) (listing examples of a continuing relationship), and (2)(ii) (listing examples of a non-continuing relationship), *see also* 12 C.F.R. § 1016.3(j)(1) (Regulation P) and (j)(2)(i).

[15] Cal. Civ. Code § 1798.140(g). This is not to be confused with CCPA's definition of a 'person' which 'means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert'. *Ibid.*, at (n). While a 'person' as defined by CCPA does not, a 'consumer' does benefit from CCPA's provision of a private right of action; CPRA does not alter CCPA's definition of either 'consumer' or 'person', but due to the addition of new definitions renumbers these definitions to Cal. Civ. Code § 1798.140(i) and (u), respectively.

[16] Much like 'Customer', GLBA's definition of 'nonpublic personal information' is fuzzy, stating only that '[t]he term "nonpublic personal information" means personally identifiable financial information'. 15 U.S.C. § 6809(4). CCPA provides a more helpful definition of 'personal information' as meaning 'information 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' but not 'publicly available information' and provides a list of specific categories of data that fall within the definition. Cal. Civ. Code § 1798.140(o). Given that CCPA only omits the word 'financial' because it is a statute of broader scope, and any hair-splitting based on these definitions has no effect on the security of the data held by a bank on a Customer, such data will be judged pursuant to CCPA's definition and simply called personal information in this article. CPRA adds a new category to CCPA's personal information by further defining 'sensitive personal information' as a narrower subset of personal information. Cal. Civ. Code § 1798.140(ae). While clarifying, and perhaps broadening, the definition of information protected under CCPA, these definitional adjustments do not affect CCPA/CPRA's private right of action and as a result have no material effect on this article's analysis of applicable data security standards.

[17] While federal Regulation S-P does in fact set forth '[p]rocedures to safeguard customer records and information … ' (17 CFR § 248.30) it limits the scope of § 248.30 to apply 'only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below. This subpart does not apply to information about companies or about individuals who obtain financial products or services primarily for business, commercial, or agricultural purposes'. 17 CFR § 248.1(b). Reg S-P does except § 248.30(b) from this definition of scope, but § 248.30(b) addresses the '[d]isposal of consumer report information and records' and 'consumer' is defined in Reg S-P as 'an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative'. Regarding family trusts not being Customers under GLBA, the Federal Trade Commission has stated that 'when a financial institution serves as a trustee of a trust, neither the grantor nor the beneficiary is a consumer or customer under the [disclosures] rule. Instead, the trust itself is the institution's "customer" and, therefore, the rule does not apply because the trust is not an individual'. Millwrights Local 1102 Supplemental Pension Fund v. Lynch, No. 07-15150, 2010 BL 158433, 2010 Us Dist Lexis 69852, 2010 WL 2772443 (E.D. Mich. 13 July 2010), Court Opinion at s. A.1. (citing Federal Register/Vol. 65, 101/24 May 2000/Rules and Regulations 33646 at 33652 while distinguishing *Chao v. Community Trust Co.*, 474 F.3d 75 (3rd Cir. 2007) which held that a trustee who was 'the legal representative of individuals who receive benefits" was a consumer under GLBA).
The Federal Trade Commission (FTC) has broad jurisdiction over cybersecurity issues, but primarily narrows its focus on when companies over-promise and under-deliver on cybersecurity and does not provide actual cybersecurity regulations. *See generally: FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 252 (3d Cir. 2015) ('there is no FTC rule or adjudication about cybersecurity that merits deference here'.). *But see infra* n. 69, explaining that GLBA Safeguards Rule refers to 'financial institutions over which the

Ultimately, the traditional legislative and data security rulemaking regimes of the United States Federal Government and the State of California cover two categories of California banking data:

(1) 'Customer' data is covered by GLBA
(2) 'consumer' data which is not preempted by GLBA such as data acquired from a casual automated teller machine (ATM) user, or related to marketing to a consumer who never becomes a Customer; and

A third category of data is not addressed by the traditional legislative and data security rulemaking regimes of the United States Federal Government and the State of California.

(3) 'Zombie Data' not of a natural person, covered neither by GLBA nor CCPA

Further, even if GLBA preempts the right of individual California residents to access or delete data collected from them by a bank, CCPA still allows a private right of action if that data is compromised,[18] and such an action will be evaluated under data security standards adopted under the laws, regulations, and jurisprudence of California.

3 What data security requirements apply to retail banks operating in California?

A retail bank operating in California is subjected to a *minimum* of three[19] data security regimes: that adopted by GLBA; that adopted by CCPA; and soft law, or rulemaking outside of the standard legislative and rulemaking processes[20] providing standards that in addition to considering personal information apply to Zombie Data not covered by GLBA or CCPA.

3.1 *CCPA*[21]

While CCPA does not set forth a data security standard within its four corners, it is enforced by the Office of the Attorney General for the State of California,[22] and that office previously commissioned a California Data Breach Report[23] which specifically adopts the Center for Internet Security's Critical Controls[24] which is a series of twenty control frameworks (Center for Internet Security's Critical Controls (CIS) 20 Controls). The CIS 20 Controls are organized as follows[25]:

Basic CIS Controls

(1) Inventory and Control of Hardware Assets
(2) Inventory and Control of Software Assets
(3) Continuous Vulnerability Management
(4) Controlled Use of Administrative Privileges
(5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
(6) Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

(7) Email and Web Browser Protections
(8) Malware Defences

Notes

[FTC] has jurisdiction'.
It can be concluded that the security of Zombie Data is not directly addressed by any California or federal statute or regulation.

18 *See* discussion *supra* nn. 9 and 10 and accompanying text.

19 (1) GLBA Safeguards Rule, *infra* n. 65; (2) CIS 20 Controls, *infra* n. 24; (3) at least one soft law standard for Zombie Data, *infra* nn. 78–90.

20 While the term 'soft law' is usually associated with international regulation, as a general concept it need not cross, or apply to multiple international jurisdictions. Marchant & Allenby define soft law as 'instruments or arrangements that create substantive expectations that are not directly enforceable, unlike "hard law" requirements such as treaties and statutes, … but nevertheless create powerful expectations'. Gary E. Marchant & Brad Allenby, *Soft Law: New Tools for Governing New Technologies*, 73 Bull. Atomic Scientists 108, 112, 109 (2017). University of Minnesota Law Professor William McGeveran calls what is referred to as soft law in this article as 'Private Ordering Frameworks', William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1158 (2019) ('private ordering – frameworks crafted primarily or entirely by industry, from the bottom up, rather than by government, from the top down').

21 An example of a state data security standard applicable to a state-chartered bank not in California would be the New York Department of Financial Services (DFS) 'Cybersecurity Regulations' (2017) applicable to banks with New York charters, but not federal charters. 23 NYCRR 500 et seq. However, for federally chartered banks based in New York it appears the DFS and the federal Office of the Comptroller of the Currency (OCC) work in conjunction making the DFS regulation informative for federally chartered banks. The New York regulations, https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations/guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default) (accessed 19 July 2021).

22 One of the most meaningful changes to CCPA implemented by CPRA is the establishment of the California Privacy Protection Agency ('CPPA'). Cal. Civ. Code § 1798.199.10 (as amended by CPRA). This means that upon full implementation of CPRA the Office of the Attorney General of the State of California will no longer be the primary enforcement agency for CCPA. The CPPA *could* abandon the CIS 20 Controls adopted by the Attorney General's Office in its California Data Breach Report discussed immediately *infra* and adopt its own data security standard(s) either through formal rulemaking or simply through its enforcement choices. But banks subject to CCPA could have nearly two years before such an adjustment in data security standards could be in effect. It is also important to note that while CCPA relies on its private right of action as the primary enforcement mechanism, CPRA continues the administrative enforcement provisions found in CCPA including fines 'of not more than two thousand five hundred dollars … for each violation, or seven thousand five hundred dollars … for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor or other person has actual knowledge is under [sixteen] years of age … ' Cal. Civ. Code § 1798.155(a) (as amended by CPRA). CPRA has retained the statutory 'damages in the amount not less than one hundred dollars … and not greater than seven hundred and fifty … per consumer per incident or actual damages'. That CPRA's new administrative remedies are in excess of ten times as high, and given the effect of the developments in federal standing jurisprudence discussed herein at s. 3.1.1, enforcement concerns for banks subject to CCPA could shift from the private right of action to administrative action if the newly formed CPPA proves to be an aggressive enforcer of CPRA.

23 Kamala D. Harris, *California Data Breach Report* (Feb. 2016), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (accessed 19 July 2021).

24 The Data Breach Report does not refer to a specific version of the CIS Controls. *Ibid.*, at v. The current version of the CIS 20 Controls is 7.1. Ctr. for Internet Sec. The CIS Controls (version 7.1 2019), https://www.cisecurity.org/controls/cis-controls-list/ (accessed 19 July 2021).

25 *Ibid* .

(9) Limitation and Control of Network Ports, Protocols and Services
(10) Data Recovery Capabilities
(11) Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
(12) Boundary defence
(13) Data Protection
(14) Controlled Access Based on the Need to Know
(15) Wireless Access Control
(16) Account Monitoring and Control

Organizational CIS Controls

(17) Implement a Security Awareness and Training Program
(18) Application Software Security
(19) Incident Response and Management
(20) Penetration Tests and Red Team Exercises

The Center for Internet Security further illuminates each of these controls with an explanation as to why the control is critical, and then provides list of sub-controls in table form with an indication of which Implementation Group should implement what sub-controls.[26] The CIS defines three of these Implementation Groups[27]:

(1) An organization with limited resources and cyber-security expertise available to implement Sub-Controls;
(2) An organization with moderate resources and cybersecurity expertise to implement Sub-Controls; and
(3) A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls.

While it could be argued that a small bank which barely qualifies as subject to CCPA may fall within CIS's Implementation Group 2, the CIS Controls further direct the consideration of 'data sensitivity' when determining a bank's appropriate implementation group.[28] Given the sensitivity of the financial data held by a bank it should be assumed that banks fall into Implementation Group 3 and have to implement each of the sub-controls set forth under each of the twenty Controls.

3.1.1 *How CCPA's Data Security Requirements Are Applied Procedurally Underwent a Drastic Change in June of 2021*

The private right of action found in CCPA sounds in negligence[29]:

– DUTY: 'the business' … duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information'
– BREACH: 'Any consumer whose nonencrypted and nonredacted personal information, … is subject to an unauthorized access and exfiltration, theft, or disclosure'
– CAUSATION: 'as a result of the business' violation of the duty to implement and maintain reasonable security practices and procedures … '
– DAMAGES: 'recover damages in an amount not less than one hundred dollars (USD 100) and not greater than seven hundred and fifty (USD 750) per consumer per incident or actual damages, whichever is greater'

However, CCPA does not address specific procedures to be used by a court hearing a private right of action brought pursuant the statute. How will private rights of action brought under CCPA be addressed by courts, thus affecting how an applicable data security standard will be adopted as the law of the case? Lacking controlling rules of civil procedure, a federal court has discretion of how to procedurally address an action.[30] Since CCPA's effective date of 1 January 2020 and as of 1 July 2021 there have been eighty suits filed making a claim pursuant to CCPA's private right of action based on a data breach: fifty-nine federal class action suits, eleven federal individual actions,[31] and ten state court actions naming in total forty-nine primary defendants arising out of forty-eight different data security incidents. The representative and single plaintiffs have asserted various combination of claims included the following eight categories:

(1) Negligence
(2) Negligence Per Se
(3) Breach of Express Contract
(4) Breach of Implied Contract
(5) Unjust Enrichment
(6) Private Right of Action as provided under § 1798.150 of CCPA

Notes

[26] *Ibid.*, at 8–70.

[27] *Ibid.*, at 4–5.

[28] *Ibid.*, at 4.

[29] *See* Cal. Civ. Code § 1798.150(a).

[30] Fed. R. Civ. P. 83(b) ('Procedure When There Is No Controlling Law. A judge may regulate practice in any manner consistent with federal law, … and the district's local rules'); *Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.*, 982 F.2d 363 (Ninth Cir. 1992) ('Courts are invested with inherent powers that are "governed not by rule or statute but by the control necessarily vested in courts to manage their own affairs so as to achieve the orderly and expeditious disposition of cases".) (*quoting Chambers v. NASCO, Inc.*, 501 U.S. 32, 41, 111 S.Ct. 2123, 2132, 115 L.Ed.2d 27 (1991)) (citation omitted).

[31] Nine of these non-class federal actions were filed by against a single defendant, Bank of America.

(7) Failure to Warn and Product Defect[32]
(8) Other causes of action than those listed above including unfair competition

Looking at these eighty CCPA private rights of action based on data security incidents involving data breaches at forty-nine different defendants that led to the loss of consumer personal information, we can see that while CCPA's private right of action appears to mimic a negligence cause of action, sixty-seven of the class representatives and single plaintiffs have separately plead a negligence cause of action, and a further twenty-two of those plaintiffs have filed a negligence per se[33] cause of action based in the violation of CCPA's data security requirement in addition to their private right of action claims arising directly out of CCPA.

As of 1 July 2021 a survey of the five unpublished rulings in pending cases featuring a CCPA private rights of action shows expected activity:

– In *McCoy v. Alphabet*[34] the CCPA private right of action did not survive a motion to dismiss as '[a]t the hearing, plaintiff conceded that this claim should be dismissed because there are no allegations of a security breach in this case'.
– In *Shay v. Apple*[35] all CCPA and negligence claims were dismissed as the plaintiff failed to oppose the motion to dismiss those claims.
– In *Gershfield v. Teamviewer*[36] plaintiff's motion to remand to state court from federal court after defendant removed was denied when defendant plausibly showed that the amount in controversy exceeded USD 5,000,000.[37] After an amended complaint was removed the court again denied a motion to remand stating that circuit courts 'have unanimously and repeatedly held that whether remand is proper [in [Class Action Fairness Act of 2005] CAFA cases] must be ascertained on the basis of the pleadings at the time of removal'. *Broadway Grill, Inc. v. Visa Inc.*, 856 F.3d 1274, 1277 (Ninth Cir. 2017). Courts ordinarily do not permit 'post-removal amendment of the complaint to affect the existence of federal jurisdiction', especially when the amendment would alter 'the make up of the class'.[38]
– In *Maag v. US Bank* a motion to dismiss was denied as moot when the court recognized a first amended complaint.[39]
– In *Gardiner v. Walmart* a motion to dismiss CCPA claims was granted based on the alleged breach being prior to the effective date of CCPA and plaintiff's failure to aver that his personal information was disclosed.[40]

It seems safe to assume that any data security standard adopted by CCPA and applied by way of its private cause of action, whether under CCPA-based private cause of action itself or an accompanying cause of action sounding in negligence will ultimately be addressed as a standard of care to which the defendant needed to rise in order to meet its duty of care 'to implement and maintain reasonable security procedures and practices appropriate to the nature of the

Notes

[32] The facts of the nineteen suits filed against Bank of America arise from allegations that prepaid debit cards provided by Bank of America pursuant to a contract with the California Employment Development Department as a method to distribute unemployment insurance benefits to eligible citizens of California were not secure and plaintiffs' benefits were funneled away by criminals able to exploit the alleged security weaknesses. Among other causes of action, the plaintiffs in these cases bring product defect claims based on the provided debit cards being a product, and the lack of a chip in addition to the magnetic stripe on the cards being a product defect which lead to data breaches. Accompanying these product liability claims are the traditional negligent failure to warn claims prevalent in product liability litigation. *See e.g.*, *Talia v. Bank of America*, Case 3:21-cv-0076-JLS-NLS compliant filed 15 Apr. 2021 in the Southern District of California at causes of action 6 and 7. The author is unaware of any action that attempts to define a non-tangible financial or non-financial service as a 'product' but it will be interesting to see if success with this tactic against Bank of America leads to an attempt by future plaintiff to allege that something like an online service such as a savings or demand deposit account is a defective product triggering the strict liability in design and operation found in product liability law in the event of a data breach.

[33] California codified the negligence per se doctrine in Evidence Code s. 669 which states in relevant part that '(a) The failure of a person to exercise due care is presumed if: (1) He violated a statute, ordinance, or regulation of a public entity; (2) The violation proximately caused … injury to person or property; (3) The … injury resulted from an occurrence of the nature which the statute, ordinance, or regulation was designed to prevent; and (4) The person suffering … the injury to his person or property was one of the class of persons for whose protection the statute, ordinance, or regulation was adopted', with the first two of these elements ordinarily reserved for the trier of fact, and the second two as matters of law being decided by the court. *Ramirez v. Nelson*, 44 Cal. Fourth 908, 918, 80 Cal.Rptr.3d 728, 188 P.3d 659 (2018) (citations omitted). Given that a duty to 'implement and maintain reasonable security procedures' only appears in the private right of action of CCPA, loss of personal information by way of a data breach may raise a genuine question as to whether a defendant who suffered a data breach violated the statute such that negligence per se applies. In the case it is found to not be such a statutory violation plaintiffs will be forced to rely on traditional negligence, but if a trier of fact holds that suffering a breach is indeed a breach of CCPA, then it appears negligence per se will be applicable as the second element will fall into place, and a plaintiff whose personal information was compromised is clearly a member of the class of person to be protected by CCPA as the loss of personal information is precisely what CCPA's private right of action was meant to prevent.

[34] *McCoy v. Alphabet, Inc.*, no. 20-cv-05427-SVK, 2021 BL 44166, 2021 WL 405816 (N. D. Cal. 2 Feb. 2021), Court Opinion at 11.

[35] *Shay v. Apple Inc.*, no. 20cv1629-GPC(BLM), 2021 BL 6143, 2021 WL 75690 (S. D. Cal. 8 Jan. 2021), Court Opinion at 10–11.

[36] *Gershfield v. Teamviewer US, Inc.*, no. SACV 21- 00058- CJC(ADSx), 2021 BL 79109, 2021 Us Dist Lexis 41931 (C.D. Cal. 4 Mar. 2021), Court Opinion.

[37] *Ibid.*, at 2–3 citing *Korn v. Polo Ralph Lauren Corp.*, 536 F. Supp. 2d 1199, 1205 (E.D. Cal. 2008) ('[C]ourts may consider the maximum statutory penalty available in determining whether the jurisdictional amount in controversy requirement is met'.); *see also* 28 U.S.C. § 1332(d)(2) for the requirements that 'the matter in controversy exceed the sum or value of [five million dollars], exclusive of interests and costs' for a class action to find diversity jurisdiction in federal court.

[38] *Gershfield v. Teamviewer US, Inc.*, *supra* n. 36, (C.D. Cal. 20 Apr. 2021), Court Opinion (citing *Broadway Grill, Inc. v. Visa Inc.*, 856 F.3d 1274, 1277–1278 (Ninth Cir. 2017)).

[39] *Maag v. U.S. Bank, N.A.*, no. 21-cv-00031-H-LL, 2021 BL 37151 (S.D. Cal. 3 Feb. 2021), Court Opinion at 1.

[40] Gardiner *v.* Walmart Inc., no. 20-cv-04618-JSW, 2021 BL 143352 (N. D. Cal. 5 Mar. 2021), Court Opinion.

information to protect the personal information'.[41] As a result, the applicable data security standard will be presented to the trier of fact by way of a battle of expert witnesses opining as to the applicable industry standard, and the reasonableness of the defendant's security safeguards, all without necessarily looking to the CIS 20 Controls.

But in June of 2021 the Supreme Court of the United States issued two decisions that may and will affect CCPA private right of action jurisprudence respectively.

First, in *Van Buren v. United States*[42] the Supreme Court held that 'exceeds authorized access' as that phrase is defined in the context of the Computer Fraud and Abuse Act of 1986[43] (CFAA) to mean that 'to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter'[44] is only triggered when a person 'accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders, or databases – that are off limits to him', but is not triggered when a person does 'not "excee[d] authorized access" to the database' in question.[45] In other words, if you have been granted access to a database, but violate policy and misappropriate personal information from that database, it is not a violation of the CFAA.

The holding in *Van Buren* may provide authority for the argument that 'is subject to an unauthorized access and exfiltration, theft, or disclosure' as used in CCPA[46] may not be triggered if an access, exfiltration, theft, or disclosure is undertaken by someone who had been granted access to the data in questions, i.e., an insider. Surely, crafty counsel for both criminal defendants under the CFAA and defendants of private rights of action under CCPA will try argue that obtaining access rights to a database by subterfuge, in other words obtaining authentic usernames and passwords by inauthentic means should still be considered as 'authorized access' thus liability under CFAA does not lie and a private right of action under CCPA fails.[47] However just as likely is that California state courts will find that the status of authorize to access is precluded by obtaining such authorization by subterfuge, and that 'unauthorized access' includes when an insider violated internal policy limiting the use of otherwise valid access credentials.

Second, in the face the Supreme Court's Article III standing decision in *Spokeo*,[48] while recognizing the *Spokeo* decision existed, the position of the Ninth Circuit Court of Appeals rule on standing as applied to cases involving data breaches has been that a plaintiff threatened with future injury has standing to sue 'if the threatened injury is "certainly impending", or there is a "substantial risk that the harm will occur"'.[49] The *Zappos* court specifically recognized that the instant plaintiff's allegation 'that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of "phishing" and "pharming", which are ways for hackers to exploit information they already have to get even more [personal information]' was sufficient to support Article III standing in federal court.[50]

In the CCPA private right of action case *Stasi v. Inmediata Health Grp. Corp.*[51] the District Court rejected the argument that '[p]laintiffs merely allege that it should be inferred or rebuttably presumed that their information was accessed by an unauthorized individual' and denied defendant's motion to dismiss the CCPA private right of action claim based on plaintiff's sufficient allegation that their information 'was viewed by unauthorized persons'. In what will surely be the basis of

Notes

[41] Cal. Civ. Code § 1798.150(a).

[42] *Van Buren, supra* n. 1.

[43] 18 U.S.C. § 1030(a)(2).

[44] 18 U.S.C. § 1030(e)(6).

[45] *Van Buren, supra* n. 1, at 20.

[46] Cal. Civ. Code § 1798.150(a)(1).

[47] *See generally* commentary by Professor Orin Kerr: 'One way to read *Van Buren* – not the only way, but the way that seems most plausible to me at this point – is that it does the major conceptual work of reining in the CFAA by casting it properly as a trespass statute. It now leaves to lower courts the largely interstitial work of figuring out the hard line-drawing of what exactly counts as enough of a closed gate to trigger liability. The authentication test suggested in [n.] 9 is one way to do it. And I personally tend to think it's the right way … But whatever the specific right answer is, the Court has now directed lower courts to the right question'. Orin Kerr, *The Supreme Court Reins in the CFAA in Van Buren*, Lawfare Blog (9 June 2021), https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren (accessed 19 July 2021).

[48] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547, 194 L. Ed. 2d 635 (2016).

[49] *In Re Zappos.com, Inc., Customer Data Sec. Breach Litig.*, 888 F.3d 1020, 1024 (Ninth Cir. 2018) (citing *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341, 189 L. Ed. 2d 246 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414, 133 S. Ct. 1138, 185 L.Ed. 2d 264 & n. 5 (2013)) (internal quotation marks omitted). *See generally*, Devin Urness, *The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution*, 73 Vand. L. Rev. 1517, 1531–1532 (2020) (stating after *Spokeo* but prior to *TransUnion* 'Divergent results in the circuits over whether the risk of future identity theft is sufficient to confer standing is not new; it has been developing since 2011. As it stands, the ... Third, Fourth, and Eighth Circuits have declined to extend standing based on a substantial risk of injury after an alleged breach. On the other hand, the D.C., Sixth, Seventh, and Ninth Circuits have found that the post-breach risk of injury is a substantial risk sufficient to establish standing'.) (footnotes with citations omitted); *see also Morris v. Carlos Lopez & Assoc., LLC,* 995 F.3d 295, 300–01 (Second Cir. 2021) (placing the Second Circuit into the post-breach risk of injury group along with the D.C., Sixth, Seventh, and Ninth Circuits).

[50] *Ibid.*, at 1027.

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

a motion to reconsider post-*TransUnion*[52] the *Stasi* court stated that defendant '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[53]:

> [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[.]'

But the Supreme Court does clear damage to the ability to litigate a CCPA private right of action in federal court with its *TransUnion v. Ramirez* decision.[54] In 2016 the Supreme Court in *Spokeo v. Robins*[55] tightened up federal standing requirements based on statutory rights of action by requiring a concrete injury 'even in the context of a statutory violation' stating that a plaintiff does not 'automatically satisf[y] 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'.[56]

Now, in *TransUnion*, the Court has eviscerated statutory causes of action as a naked basis for federal standing[57]:

> For standing purposes, therefore, an important difference exists between (i) a plaintiff's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff's suffering concrete harm because of the defendant's violation of federal law. Congress may enact legal prohibitions and obligations. And Congress may create causes of action for plaintiffs to sue defendants who violate those legal prohibitions or obligations. But under Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court.

There is no reason to believe that the holding of *TransUnion* does not apply to statutory causes of action created by state law such as CCPA's private right of action, thus in federal court, CCPA private right of action plaintiffs will no longer survive an attack based on standing without at least making a colourable argument that they have been 'concretely' harmed – a requirement which the private right of action was meant to provide by way of its statutory damages.[58] With 87.5% of breach-based CCPA actions being in federal court as of 1 July 2021, one can predict the chilling effect of the *TransUnion* decision on claims arising from CCPA's private right of action.

In his dissent in *TransUnion*, Justice Thomas states the following[59]:

> Today's decision might actually be a pyrrhic victory for TransUnion. The Court does not prohibit Congress from creating statutory rights for consumers; it simply holds that federal courts lack jurisdiction to hear some of these cases. That combination may leave state courts – which 'are not bound by the limitations of a case or controversy or other federal rules of justiciability even when they address issues of federal law', … as the sole forum for such cases, with defendants unable to seek removal to federal court. … By declaring that federal courts lack jurisdiction, the Court has thus ensured that state courts will exercise exclusive jurisdiction over these sorts of class actions.

Justice Thomas's comments are well-taken, but as discussed *supra*, the seventy federal court actions making a claim based on the CCPA's private right of action also make other claims, including common law claims which remain justiciable in federal court between diverse parties.[60] This leads to the conclusion that a CCPA right of action can easily be dispatched by a California-diverse defendant merely by removing the overarching action to federal court.

Notes

[52] *See* discussion immediately *infra*, of *TransUnion, supra* n. 2.

[53] *Stasi, supra* n. 51, at 20.

[54] *TransUnion, supra* n. 2.

[55] *Spokeo, supra* n. 48.

[56] *Ibid.*, at 1549.

[57] *TransUnion*, *supra* n. 2, at 11.

[58] Urness, *supra* n. 49, at 1519 (stating regarding standing in data breach cases prior to *TransUnion*: 'If a claim is based on a private right of action in a statute, plaintiffs who may otherwise have insufficient evidence to create an injury in fact can rely on Congress's definition of what constitutes an injury'.).

[59] *TransUnion, supra* n. 2, J. Thomas in dissent at 18, n. 9.

[60] It should be noted that none of the eighty CCPA private right of action bearing cases filed as a result of data breaches from 1 Jan. 2020 to 1 July 2021 allege a cause of action that would support federal jurisdiction under 28 U.S.C. § 1441(a), with each cause of action being based in common law or state statute. *See generally, infra* n. 75, regarding no private right of action arising out of GLBA but GLBA supporting a negligence per se cause or action.

Or can it?[61] Whether a theory of fraudulent removal will successfully prevent the dismissal of CCPA private rights of action by way of removal will depend on strategic pleading and will be reviewed on a case-by-case basis and is beyond the scope of this article and is mentioned as a launch pad for further investigation.

What about California-based defendants that cannot rely on diversity as a basis for removal? Due to the lack of claims over which federal courts have original jurisdiction, non-diverse defendants will not be able to use *TransUnion* to kill CCPA private right of action claims by first removing then moving to dismiss.[62] But for the rare case of a plaintiff whose private right of action under CCPA accrued while they were residents of California, but who moved to the state in which the plaintiff is domiciled prior to filing their action, the very nature of CCPA only extending to residents of California[63] appears to allow any non-California-based defendant to be able to defeat a CCPA private right of action claim by removing the action and relying on *TransUnion*.

Ultimately, if *Van Buren* serves as a picador and *TransUnion* a toreador striking a fatal blow to CCPA's private right of action for diverse defendants the argument for the CIS 20 Controls being the applicable data security standard applicable to banks operating in California strengthens as enforcement duties will necessarily default to the Attorney General's office currently, and the newly formed California Privacy Protection Agency in the future, and as discussed *supra*, these bodies surely will adopt the CIS 20 Controls as the applicable standard of care.[64]

3.2 *GLBA*

GLBA has a 'Safeguards Rule' initially adopted in 2002 which currently sets forth five areas of control.[65] The Safeguards Rule, as flushed out in the Code of Federal Regulations (CFR), is currently undergoing a regulatory amendment procedure, the conclusion of which will result in significant amendments to the associated CFRs.[66]

Unlike the CIS 20 Controls, GLBA Safeguards Rule provides a very general description of a mandatory data security program. The Safeguards Rule states that in order to further a financial institution's obligation to respect the privacy of its Customers,[67] regulatory agencies shall establish standards within:

> their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) To ensure the security and confidentiality of Customer records and information;
> (2) To protect again any anticipated threats or hazards to the security or integrity of such records; and
> (3) To protect against unauthorized access to or use of such records or information which could result in substantial harm of inconvenience to any Customer.[68]

The CFRs augment the Safeguards Rule by first stating[69]:

> [the Rule] sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Mimicking but expanding on the statute, the CFR goes on to define an information security program as:

> the administrative, technical, or physical safeguards [a financial institution] uses to access, collect, distribute,

Notes

[61] There is a theory that could potentially give CCPA private right of action plaintiffs ammunition in a fight to keep a diverse defendant from removing their action: 'Fraudulent removal occurs when a defendant removes a case to federal court asserting any basis of federal jurisdiction that is made in bad faith or is wholly insubstantial. Perhaps the clearest example of fraudulent removal is when a defendant removes a case to federal court although it plans to seek immediate dismissal based on lack of subject matter jurisdiction. This self-incriminating motion shows that defendant knew or should have known that removal was improper'. Zachary D. Clopton & Alexandra D. Lahav, *Fraudulent Removal*, 135 Harv. L. Rev. F. forthcoming, Northwestern Public Law Research Paper no. 21-15, SSRN (3 June 2021), https://ssrn.com/abstract=3858677 (accessed 19 July 2021).

[62] Thirteen of the data breach-based actions filed from 1 Jan. 2020 through 1 July 2021 and including a CCPA private right of action have been filed in federal district courts outside of California. *See* e.g., *Hood et al. v. U.S. Bancorp*, 0:20-cv-02101-DSD-KMM filed 2 Oct. 2020 and *Marcaurel v. Waste-Mgmt.*, 4:21-cv-02027 filed 21 June 2021 with each of these actions alleging two classes: a nationwide class, and a subclass of those plaintiffs residing in the State of Cal.

[63] *See* Cal. Civ. Code § 1798.140(g).

[64] *See supra*, n. 22, for discussion of the enforcement agencies of CCPA and CPRA; CIS 20 Controls, *supra* n. 24.

[65] 16 C.F.R. pt. 314.

[66] Amendment to the Safeguards Rule were initially proposed 4 Apr. 2019 with a public comment deadline of 2 Aug. 2019 via Project no. 145407 with Docket Number: FTC-2-19-0019, https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information#citation-3-p13159 (accessed 19 July 2021), with the docket for the progress of the amendments, https://beta.regulations.gov/document/FTC-2019-0019-0011 (accessed 19 July 2021). Analysis of when the proposed amendment to the GLBA Safeguards Rule could be adopted is beyond the scope of this article, but the amendment could be adopted at any time. *See generally*, Administrative Conference of the US, *Hybrid Rulemaking Procedures for the Federal Trade Commission*, https://www.acus.gov/recommendation/hybrid-rulemaking-procedures-federal-trade-commission (accessed 19 July 2021).

[67] *See supra* n. 14, regarding the definition of 'Customer' meaning an individual.

[68] 15 U.S.C. § 6801(b).

[69] 16 CFR § 314.1(a). Interestingly, § 314.1(b) which addresses scope, indicates '[t]his part applies to the handling of customer information by all financial institutions over which the [FTC] has jurisdiction' instead of calling out a more focused regulator of financial institutions such as the Office of the Comptroller of the Currency.

process, protect, stores, use, transmit, dispose or, or otherwise handle customer information.[70]

Such an information security program is to be 'written in one or more readily accessible parts and contain[] administrative, technical, and physical safeguards that are appropriate to [the financial institution's] size and complexity, the nature and scope of [the institution's] activities, and the sensitivity of any customer information at issue' with the aim of meeting the objectives set forth in the statute.[71]

The information security program required by the Safeguards Rule must address a specific list of elements. A financial institution shall:

(a) Designate an employee to coordinate the program.
(b) Identify reasonably foreseeable internal and external risks to the security which could allow unauthorized disclosure, misuse, alteration, destruction or other compromise to customer information. At a minimum this risk assessment should consider each relevant area of operations, including:
    (1) Employee training and management;
    (2) Information systems, including network and software design, information processing, storage, transmission, and disposal; and
    (3) Detecting, preventing and responding to attacks, intrusions, or other system failures.
(c) Design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' controls, systems, and procedures.[72]
(d) Oversee service providers, by[73]:
    (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards; and
    (1) Requiring service providers by contract to implement and maintain such safeguards.
(e) Evaluate and adjust the information security program in light of results of testing and monitoring, material changes to operations or business arrangements, or any other circumstance that are known or the financial service institution has reason to know may have a materials impact on the program.[74]

While the current version of the Safeguards Rule is almost airy in its brevity, the proposed Amendments to the Rule closely track the CIS 20 Controls favoured by the California Attorney General's Office. The GLBA does not provide a statutory private right of action, but the Safeguards Rule has been found to support a negligence per se claim.[75]

3.3 *Soft Law*[76]

A bank operating in California and handling Zombie Data must ultimately rely on Soft Law data security standards for guidance. While there are many more standards than those set forth herein,[77] these are the standards most directly applicable to banks:

(1) Federal Financial Institution Examination Council (FFIEC) Cybersecurity Assessment Tool 'comprises the principles of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee'.[78] The Assessment Tool presents five Domains and Assessment Factors and defines five maturity levels.
(2) As more and more institutions are insuring against cybersecurity related risk, the National Association of Insurance Commissioners 'Model Law' (2017), which is an adoption of a now disbanded

Notes

[70] 16 CFR § 314.2(c).

[71] 16 CFR § 314.3.

[72] The primary addition proposed by the Amendments to the Safeguards Rule are the addition of ten subss to this design and implement mandate including: (1) access controls; (2) business objectives of data; (3) restriction of physical access; (4) encryption; (5) secure development practices for software; (6) multi-factor authentication; (7) audit trails; (8) data disposal procedures; (9) change management; and (10) policies, procedures, and controls. 16 CFR § 314.4(c)(1)-(10).

[73] The other significant addition proposed by the Amendments to the Safeguards Rule is the addition of a new subss d and e (the current d is renumbered as f) that cover updated requirements regarding requirements to '(d) Regularly test or otherwise monitor the effectiveness of the safeguard's key controls, systems, and procedures … ' (including annual penetration testing) and '(e) Implement policies and procedures to ensure personnel are able to enact [the] information security program … ' *Ibid.*, at § 314.4(d)-(e).

[74] *Ibid.*

[75] *USAA Fed. Sav. Bank v. PLS Fin. Servs., Inc.*, 340 F. Supp. 3d 721, 726 (N.D. Ill. 2018) ('it is well-recognized that the GLBA does not provide a private right of action'); *but see In Re Equifax, Inc. Cust. Data Security Breach Litigation*, 371 F.Supp. 3d 1150, 1174 (N.D. Ga. 2019) (applying Georgia law to hold that 'unlike GLBA itself, the Court concludes that the Safeguards Rule provides and ascertainable standard of conduct permitting it to serve as the basis for a negligence per se claim'.).

[76] *See supra* n. 20, for a definition of the term Soft Law.

[77] *See generally*, McGeveran, *supra* n. 20, at 1139 (addressing 'fourteen different "frameworks" that impose data security obligations on private companies', including seven that fall into the Soft Law category).

[78] FFIEC, *FFIEC Cybersecurity Assessment Tool* (2017), n. 1, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf (accessed 19 July 2021).

Cybersecurity Working Group, could become more important as in addition to meeting statutory requirements institutions seek to appease potential insurers.[79] The Model Law adopted five items:

(a) Principles for Effective Cybersecurity: Insurance Regulatory Guidance[80];
(b) Roadmap for Cybersecurity Consumer Protections[81];
(c) Financial Conditions Examiners Handbook (with revised cybersecurity protocols)[82];
(d) Market Regulation handbook[83]; and
(e) Insurance Data Security Model Law.[84]

(3) As most banks facilitate credit and debit card payment, the Payment Card Industry – Data Security Standards (PCI-DSS) are applicable. A prioritized approach to the standard is arranged as a series of milestones, goals, and twelve requirements.[85]
(4) The non-profit, self-regulatory Financial Industry Regulatory Authority (FINRA) has issued a Report on Cybersecurity Practices (2015)[86] requiring licensed brokers to maintain certain security measures which 'are consistent with SEC requirements under the Safeguards Rule but are more demanding'.[87]
(5) Finally, the National Institute of Standards and Technology (NIST) has promulgated the gold standard[88] of data security standards with its NIST Framework for Improving Critical Infrastructure Cybersecurity[89] v1.1 (2018) which is as its name suggests a forty-six-page framework relying on reference to the behemoth 462-page NIST 800-53r5 Security and Privacy Controls for Information Systems and Organizations for the details of what is recognized as a leading industry standard for data security.[90]

4 How can a bank operating in California meet all applicable data security requirements?

As discussed above, the data security regulations to which a bank operating in California are not clear, and in any event, there is no 'certification' that a bank can use as a shield to show they have met the applicable data security requirements. However, when one looks deeper into the data security standards mentioned in this article, it can be seen that they are an incestuous group of standards. The California Data Breach report specifically calls out the NIST Framework and NIST 800-53 as foundational.[91] The CIS 20 Controls specifically list the NIST Framework as support material.[92] Each function of the NIST Framework lists the corresponding CIS 20 Control as an informative reference.[93] The FFIEC Cybersecurity

Notes

[79] NAIC, *Cybersecurity* (27 May 2021), https://content.naic.org/cipr_topics/topic_cybersecurity.htm (accessed 19 July 2021).

[80] NAIC, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), https://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf (accessed 19 July 2021).

[81] NAIC, *NAIC Roadmap for Cybersecurity Consumer Protections* (2015), https://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf (accessed 19 July 2021).

[82] NAIC, *Insurance Summit – 2016 Financial Condition Examiners Handbook Update* (2016), https://content.naic.org/sites/default/files/inline-files/insurance_summit_160511_financial_exam_update.pdf (accessed 19 July 2021).

[83] NAIC, *Publications*, https://www.naic.org/prod_serv_alpha_listing.htm#mkt_reg_hb (accessed 19 July 2021).

[84] NAIC, *Insurance Data Security Model Law, in NAIC Model Laws, Regulations, Guidelines and Other Resources – Fourth Quarter 2017*, https://www.naic.org/store/free/MDL-668.pdf?39 (accessed 19 July 2021).

[85] PCI-DSS, *PCI-DSS Prioritized Approach to PCI-DSS 3.2.1*, https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf?agreement=true&time=1606349286526 (accessed 19 July 2021).

[86] FINRA, *Report on Cybersecurity Practices* (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (accessed 19 July 2021).

[87] McGeveran, *supra* n. 20, at 1167.

[88] Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 Conn. L. Rev. 1495, 1504–1505 (2017) ('The gold-standard for approaching security is the NIST Cybersecurity Framework').

[89] NIST, *NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1* (2018), https://www.nist.gov/system/files/documents/2018/05/14/framework_v1.1_with_markup.pdf (accessed 19 July 2021).

[90] NIST, *NIST 800-53r5 Security and Privacy Controls for Information Systems and Organizations* (Sep. 2020), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed 19 July 2021). Interestingly, 800-53r5 supersedes NIST 800-53r4 which included the extra qualifier 'Federal' in its title Security and Privacy Controls for Federal Information Systems and Organizations. Similarly, 800-53r4 included the notice that '[t]he purpose of this publication is to provide guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all components of an information system that process, store, or transmit federal information', thus specifically limiting its application to federal information systems. To the contrary, 800-53r5 changes this federal-only language to '[t]his publication establishes controls for systems and organizations. The controls can be implemented within any organization or system that processes, stores, or transmits information. The use of these controls is mandatory for federal information systems … ' This change of removing the federal-only qualification from 800-53 effects what was already a de facto application of the Standard as security professionals widely recognize NIST 800-53 as the gold standard in data security, even for systems not handling classified or non-classified information for the federal government.

[91] Harris, *supra* n. 23, at 30.

[92] CIS 20 Controls, *supra* n. 24, at 6.

[93] NIST, *supra* n. 89, at 24–44.

Assessment Tool provides an appendix which maps the Tool to the NIST Framework.[94] The PCI-DSS lists the CIS 20 Controls and NIST standards as 'industry-accepted' security standards.[95] The FINRA Report suggests that a variety of standards can be drawn upon, including the NIST Framework and PCI-DSS.[96] Even the proposed amendments to GLBA's Safeguards Rule are based in large part on the New York Department of Financial Services' 'Cybersecurity Regulations'.[97]

While it must be recognized that if an action authorized by CCPA's private right of action follows traditional negligence jurisprudence then the applicable standard of care will be set by an inefficient battle of expert witnesses, narrowing down the actual standards a bank operating in California will ultimately need to show adherence to tends to collapse on what is a 'reasonable' security program.[98]

Professor McGeveran has presciently stated that:

> [S]ome frameworks have moved away from the explicit language of 'reasonableness,' perhaps in part because of the great discomfort IT professional and other technically-oriented stakeholders express about that word. However, these frameworks continue the reliance on individual risk assessments, with the result that they function in almost the same way – because responses shaped by a proper risk assessment are, by definition, reasonable.[99]

Which brings us back full circle to the California Data Breach Report which recognizes that[100]:

> [w]hile there is no dearth of information on the security risk management process and standards for security controls, [and] synthesizing all of this information and prioritizing the actions to take can be a challenge, [the CIS 20 Controls are] designed to address this challenge.

If one's concern switches to state enforcement actions as opposed to private rights of action, it cannot be ignored that the current CCPA enforcement agency has specifically recognized the CIS 20 Controls as a reasonable data security standard.

5 Conclusion

After weaving our way through the various data security standards that will, or may apply to a retail bank operating in California in light of recent Supreme Court decision effectively precluding CCPA private rights of action in federal courts in the absence of concrete damages, we can see that given that the current regulator of CCPA has adopted the CIS 20 Controls, and in light of the respect given to the twenty Controls by other security frameworks, along with the looseness of the Safeguards Rule, that benchmarking the CIS 20 Controls appears to be the surest way to repel either state or federal administrative enforcement or private right of action based on a security breach resulting in the loss of customer personal information by a retail bank operating in California.

Notes

[94] FFIEC, *supra* n. 78, at 1 and Appendix B.

[95] PCI-DSS, *supra* n. 85, at 4.

[96] FINRA, *supra* n. 86, at 8–9.

[97] *See supra* n. 21; Dissenting Statement of Commissioners Noah Joshua Phillips & Christine S. Wilson, *Regulatory Review of Safeguards Rule*, Matter no. P145407 (5 Mar. 2019), https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf (accessed 19 July 2021).

[98] Given that CCPA's private right of action is effectively dead in federal actions featuring diversity jurisdiction, it is especially true that applicable data security standards will be argued inside negligence actions. *See supra* nn. 54–64 and accompanying text discussing the effect of the *TransUnion* decision on private right of action federal jurisdiction.

[99] McGeveran, *supra* n. 20, at 1178.

[100] Harris, *supra* n. 23, at 30.