II. The Status of Data Breach Law in Light of Capital One

A. Introduction: Why Care About Data Breach?

As the world becomes more digitized, data privacy and security have become two of businesses' top priorities as data breach incidents emerge ever more frequently. According to the Identity Theft Resource Center, in 2017, there were 1,579 data breaches in the United States, a 44.7% increase over the number reported in 2016.[1] Specifically, 8.5% of the total number of breaches in 2017, amounting to 134 incidents, were within the banking, credit, and financial sector.[2] In the past twelve years, this percentage has fluctuated around ten percent annually.[3] Notable institutions such as Equifax, Citigroup, Countrywide Financial (later acquired by Bank of America), and Ernst & Young have all had their consumers' personal and financial information stolen over a twelve-year period.[4] Generally, the harm from data breaches come in the form of "increased risk of financial injury and anxiety," but this is an intangible harm that courts do not always recognize.[5] The risk of a data breach may take years to effectuate, and the resulting harm can be permanent as people cannot change their

---

[1] Identity Theft Res. Ctr., *2017 Annual Data Breach Year-End Review* (Feb. 8, 2017), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf ("The number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, according to the 2017 Data Breach Year-End Review released by the Identity Theft Resource Center® (ITRC) and CyberScout®. The Review indicates a drastic upturn of 44.7 percent increase over the record high figures reported for 2016.").

[2] *Id*. ("The Banking/Credit/Financial sector rounds out the top three with 8.5 percent of the overall total (134).

[3] *Id.* (No text supporting this but can see from the graph/chart.).

[4] PRIVACY RIGHTS CLEARINGHOUSE, *Data Breaches* https://www.privacyrights.org/data-breaches [https://perma.cc/3PJD-GZQ8] (last visited Oct. 6, 2019) (No text but from search results using the database).

[5] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 737 (2018) ("This past term, the U.S. Supreme Court stated in Spokeo v. Robins that "intangible" injury, including the "risk" of injury, could be sufficient to establish harm. When does an increased risk of future injury and anxiety constitute harm? The answer remains unclear.").

social security numbers, birth dates, or biometric data.[6] Data breach incidents force individuals to spend time and money to monitor their financial accounts and incur emotional distress.[7] In the words of Daniel J. Solove, Professor of Law at the George Washington University Law School, and Danielle Keats Citron, Professor of Law at Boston University School of Law, "[d]ata-breach harm might often be intangible, but it still is very real."[8] It is fair to say that data breach has been a serious and well-known issue for financial institutions, even before the Capital One incident took place. This article seeks to provide a brief overview of data breach law, particularly as it relates to data breaches at financial institutions, such as the Capital One data breach. Section II of this article discusses the Capital One incident itself and its aftermath. Section III explores the status of data breach laws at the time of the incident on the federal and state levels, along with a reference to the data breach regime in Europe. Section IV summarizes this article and provides some predictions about future trends of data breach law in the United States.

B. Capital One Incident: What Happened?

Captal One is the "fifth largest consumer bank and eighth largest bank overall" in the United States.[9] In July 2019, Capital One experienced a severe data breach that affected approximately 100 million U.S. customers and six million Canadian customers.[10] Capital

---

[6] *Id.* at 757–58 ("It may take months or years before leaked personal data is abused, but when it happens, the harm can be profound.").

[7] *Id.* at 758, 764 ("Their opportunity costs are real. Individuals spend time monitoring their accounts, which pulls them away from their jobs.") ("Data-breach harms often result in victims experiencing anxiety about the increased risk of future harm. Anxiety is a form of emotional distress, which is an umbrella term to capture a wide array of negative and disruptive feelings such as sadness, embarrassment, and anxiety, among others.").

[8] *Id.* at 786 ("Data-breach harm might often be intangible, but it still is very real.").

[9] CAPITAL ONE, *Corporate Information: Our Company*. https://www.capitalone.com/about/corporate-information/our-company [https://perma.cc/RNY5-VH3E] (last visited Oct. 26, 2019) ("We are now the nation's fifth-largest consumer bank and eighth-largest bank overall.").

[10] CAPITAL ONE, *Information on the Caital One Cyber Incident* https://www.capitalone.com/facts2019/ [https://perma.cc/7S98-G2E2] (last updated Sept. 23, 2019) ("Based on our analysis to date, this event affected approximately

One announced that although "no credit card account numbers or log-in credentials were compromised," about 140,000 social security numbers and 80,000 linked bank account numbers belonging to U.S. customers, as well as about one million Social Insurance Numbers of Canadian customers, were hacked by the perpetrator.[11] More generally, the names, addresses, zip codes, phone numbers, email addresses, birth dates, and self-reported income information of the 106 million customers were also exposed.[12] The bank immediately announced that it would "notify affected individuals through a variety of channels" and "make free credit monitoring and identity protection available to everyone affected."[13]

The investigation revealed that Paige A. Thompson, a former employee of Amazon Web Services (AWS), perpetrated the hack by infiltrating Capital One's customer data stored on AWS's Simple Storage Service and taking advantage of "a firewall misconfiguration permit[ing] commands to reach and be executed by that server."[14] Capital One later announced that it had fixed the vulnerability in question and concluded that "it is unlikely that the information was

---

100 million individuals in the United States and approximately 6 million in Canada.").

[11] *Id.* ("Importantly, no credit card account numbers or log-in credentials were compromised. . . . The individual also obtained the following data:• About 140,000 Social Security numbers of our credit card customers.• About 80,000 linked bank account numbers of our secured credit card customers.").

[12] *Id.* ("The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income.").

[13] Press Release, Capital One Announces Data Security Incident (July 29, 2019) (on file at https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/) ("We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.").

[14] Jack Lu, *Assessing the Cost, Legal Fallout of Capital One Data Breach*, LAW360 (Aug. 15, 2019, 6:20 PM), https://www.law360.com/articles/1189143/assessing-the-cost-legal-fallout-of-capital-one-data-breach ('As part of the investigation, Paige A. Thompson, an ex-employee from Amazon Web Services has been arrested and accused of "intruding into the servers rented or contracted" by Capital One. Specifically, "a firewall misconfiguration permitted commands to reach and be executed by that server," which enabled the intrusion.').

used for fraud or disseminated by this individual." [15] Nevertheless, the New York State Attorney General's office initiated an investigation into the incident within twenty-four hours of the announcement of the data breach and several law firms also planned to file lawsuits against Capital One.[16] On July 30, 2019, a class action was brought against Capital One for failure to take reasonable care over customers' sensitive information in the United States District Court for the Eastern District of Virginia.[17] The bank itself estimated that the incident could incur a cost between $100 million to $150 million to cover "customer notifications, credit monitoring, technology costs and legal support."[18] Cybersecurity expert Morgan Wright, a senior fellow at the Center for Digital Government, claimed that "[t]his damage to Capital One is probably going to exceed $200 to $300 million dollars by the time it's all said and done."[19]

---

[15] *Id.* ('Capital One reported that it had "immediately fixed the configuration vulnerability that this individual exploited" and that "it is unlikely that the information was used for fraud or disseminated by this individual."').

[16] *Id.* ("Still, in less than 24 hours after Capital One announced the data breach, New York State Attorney General Letitia James' office decided to begin an investigation into the incident. Also, nearly a dozen law firms declared that they are looking into the matter and plan to file class lawsuits against Capital One on behalf of its customers and shareholders.").

[17] AJ Dellinger, *Capital One Hit with Class-Action Lawsuit Following Massive Data Breach*, FORBES (July 30, 2019, 10:30 PM), https://www.forbes.com/sites/ajdellinger/2019/07/30/capital-one-hit-with-class-action-lawsuit-following-massive-data-breach/ [https://perma.cc/S2Q7-MKLS] ("Following a massive data breach that compromised the personal information of more than 100 million people, Capital One has been hit with a class-action lawsuit. A complaint from the law firm of Morgan and Morgan was filed today with the United States District Court for the Eastern District of on behalf of the millions of consumers affected by the breach.")

[18] Capital One, *supra* note 14 ("We expect the incident to generate incremental costs of approximately $100 to $150 million in 2019. Expected costs are largely driven by customer notifications, credit monitoring, technology costs, and legal support.").

[19] Grete Suarez, *Cost of Capital One's Data Breach Could Exceed $300 million: Expert*, YAHOO FINANCE (July 30, 2019), https://finance.yahoo.com/news/cost-of-capital-ones-data-breach-could-exceed-300-million-expert-224823227.html ('"This damage to Capital One is probably going to exceed $200 to $300 million dollars by the time it's all said and done," said Morgan Wright, cybersecurity expert and senior fellow at the Center for Digital Government, on Yahoo Finance's The Ticker.').

The Capital One breach is very similar to the Equifax breach in 2017, as both were major financial institutions and the incidents involved the breach of personal financial information of at least 100 million U.S. consumers. What happened to Equifax after the breach in 2017 can be a reference for what may happen to Capital One this time. In July, the Federal Trade Commission (FTC) announced that Equifax, one of three major consumer credit reporting agencies in the United States, agreed to pay a $700 million settlement for its data breach incident in 2017.[20] Sometime during May to July of 2017, Equifax was hacked and the hack affected 145.5 million Equifax customers—nearly half of the U.S. population.[21] Similar to the Capital One incident, Equifax customers' names, social security numbers, birth dates, addresses, and driver's license numbers were compromised; more than 200,000 customers' credit card information was also exposed.[22] Notably, Equifax did not officially announce the incident until September 2017, several months after its occurrence.[23] Investigations later revealed that Equifax took several months to "install a critical software patch after the Department of Homeland Security notified them of the update," showing how slow Equifax was in responding to a potential

---

[20] Seena Gressin, *The Capital One Data Breach: Time to Check Your Credit Report*, FED. TRADE COMM'N CONSUMER INFO. BLOG (July 30, 2019), https://www.consumer.ftc.gov/blog/2019/07/capital-one-data-breach-time-check-your-credit-report [https://perma.cc/SX2J-7EUR] (". . . Equifax agreed to pay up to $700 million to settle a lawsuit brought by the FTC, the Consumer Financial Protection Bureau, and 50 states and territories, stemming from the credit reporting giant's 2017 data breach, which affected about 147 million people.").

[21] McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. OF NAT'L SEC. L. & POL. 549, 553–54. ("The Equifax hack resulted in the loss of vital information—names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers—for 143 million people, impacting nearly half the U.S. population. . . . The number would later be updated to 145.5 million Americans.").

[22] *Id.* ("The Equifax hack resulted in the loss of vital information—names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers—for 143 million people, impacting nearly half the U.S. population.").

[23] *Id.* (On September 7, 2017, Equifax, one of the largest consumer-credit reporting agencies in the world, publicly announced that its consumer information had been compromised as a result of a "cybersecurity incident.". . . The actual breach had occurred months earlier, from May 2017 to July 2017. . . .").

threat of breach even after the government gave them a warning.[24] Moreover, "[i]t took eleven weeks for Equifax's security team to even notice the suspicious network activity once their system was breached," and the credit reporting agency took a few more weeks to contact a law firm, register a domain name for customer support, and issue a press release.[25] In the end, a total of "twenty-six weeks passed from the date that the Department of Homeland Security issued its warning until Equifax finally announced that its systems had been compromised."[26] In contrast, Capital One's incident in 2019 affected less customers in the United States (100 million vs. 145.5 million) and the bank's response for announcing the incident and fixing the vulnerability was much faster.[27] This could possibly mean that the negative implications from the breach for Capital One would be less severe than for Equifax in 2017. So far this predication seems to hold true; as of July of 2019, the stock market loss for Capital One was $1.44 billion while that for Equifax came down to $5.9 billion.[28]

---

[24] *Id.* at 559. ("[I]t took Equifax several months to install a critical software patch after the Department of Homeland Security notified them of the update.").

[25] *Id.* ("It took eleven weeks for Equifax's security team to even notice the suspicious network activity once their system was breached. It took four additional days to contact a law firm and cybersecurity company for the purposes of conducting a comprehensive investigation. After three more weeks, Equifax had the foresight to register a domain name for consumer support, meaning that, at that point, they likely knew the extent of the damage. Despite that knowledge, however, it then took Equifax another two weeks to issue a press release and notify the American public that their most private information had been stolen.").

[26] *Id.* ("In total, twenty-six weeks passed from the date that the Department of Homeland Security issued its warning until Equifax finally announced that its systems had been compromised.").

[27] *See supra* Section II (discussing Capital One breach incident).

[28] Lu, *supra* note 15 ("Capital One announced the incident on July 29 after the market closed, and its stock price. . . . conveys a decline in stock market value of $1.44 billion. . . . By contrast, after announcing its data breach event in 2017, Equifax Inc. witnessed a seven-day turmoil in its stock trading . . . which translated to loss of market value of $5.9 billion.").

C. The Status of Data Breach Law: Federal, State, and Foreign

The current framework for data breach law focuses on requiring companies to notify individuals when they are affected by data breach incidents.[29] On the federal level, data breach regulations in the financial sector comprise of the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and amendments to the Sarbanes-Oxley Act (SOX).[30] Title V of the GLBA explicitly requires financial instutions to "develop procedures for protecting the security of customer data."[31] It also empowers several regulatory agencies to issue "Interagency Guidances" on maintaining reasonable data security and responding to data security breaches.[32] In addition, the FCRA specifically deals with "data brokers" (such as Equifax) by putting in place regulations on the permissible use of personal data for businesses that collect, maintain, and resell such data.[33] However, the FCRA does not have any requirement on maintaining data security.[34] Finally, section 404 of SOX requires company officers to certify the accuracy of their company's financial data and "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a

---

[29] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2006) ("The law increasingly requires private companies to disclose certain information for the benefit of consumers.").

[30] *Id.* at 920–23 (discussing relevant provisions on data security in the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Sarbanes-Oxley Act).

[31] *Id.* at 920 ("Title V of the Gramm-Leach-Bliley Act (GLB Act) requires financial institutions to develop procedures for protecting the security of customer data. . . .")

[32] *Id.* ("These agencies have, in turn, issued two "Interagency Guidances" pursuant to the GLB Act; one requires financial institutions to maintain reasonable data security, and the other requires them to develop a formal response program to deal with data security breaches.").

[33] *Id.* at 922–23 ("Data brokers are in the business of collecting personal information, maintaining it in databases, and extracting value from it by comparing and combining it with other information and then reselling it.").

[34] *Id.* ("Regardless of the extent to which the FCRA does or does not apply to the database industry, however, the FCRA itself lacks any data security requirements.").

material effect on the financial statements."[35] In sectors other than finance and business, federal laws are also in place to regulate data security.[36] For example, the Health Insurance Portability and Accountability Act (HIPAA) covers the security of patient health information, while the Family Educational Rights and Privacy Act (FERPA) covers the privacy of education information of students.[37] In addition to the regulatory protections in place, victims of privacy breaches can bring private lawsuits against companies.[38]

While the aforementioned federal laws impose some regulations on data practices of private businesses, it is worth noting that *none* of the above mentioned regulations, as applied to the financial sector, mandate notifications to individuals affected by data breach incidents;[39] rather, notifications laws are strictly in the domain of the states.[40] For consumers, notice is crucial because it "mitigat[es] harm after a data leak."[41] "In the absence of a comprehensive federal data breach notification law," consumers rely on state laws for imposing requirements on companies to notify them whenever they are affected by data breach incidents.[42] All fifty states, the District of Columbia,

---

[35] *Id.* at 923–24 ("While the focus of the certification is on the accuracy of financial reporting, one requirement is that these officers certify that these internal controls "[p]rovide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.")

[36] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 42–43 (2015) (discussing a list of federal data security laws).

[37] *Id.* ("Health Insurance Portability and Accountability Act of 1996—gives the Department of Health and Human Services the authority to promulgate regulations governing the privacy of medical records. . . Family Educational Rights and Privacy Act of 1974. . . —protects the privacy of school records.").

[38] Schwartz & Janger, *supra* note 29, at 923. ("In tort law, under a general negligence theory, litigants might sue a company after a data security incident and seek to collect damages.")

[39] HIPAA does have a notification requirement, but it only applies to medical and health information.

[40] Schwartz & Janger, *supra* note 29, at 924 ("[T]hirty-three states and one city have enacted notification legislation within a few short years.").

[41] *Id.* at 913 ("An important function of breach notification is mitigation of harm after a data leak.").

[42] GINA MARIE STEVENS, CONG. RESEARCH SERV., RL 34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2008) ("In the absence of a comprehensive federal data breach notification law, many states enacted laws requiring consumer notice of security breaches of personal data. The majority of states have introduced or passed bills to require

and other U.S. territories have enacted legislation requiring businesses to "notify individuals of security breaches of information involving personally identifiable information."[43] These laws typically have the following provisions: types of entities that must comply, scope of personal information, definition of a breach, timing and method of notice, and exemptions.[44] Some specific provisions will be discussed below.

In recent months, at least twenty-one states have been considering amending existing laws.[45] The proposed amendments focus on four areas: expanding the definitions of personal information, shortening the timeframe of reporting a breach, requiring breaches to be reported to state attorney generals, and providing free credit freezes or identifying theft protections.[46] The proposed amendments, if they come into effect, would significantly strengthen current data breach laws in those states. In New York, for example, two amendments have been enacted in 2019.[47] One amendment expanded the definition of personal information beyond the traditional categories of social security numbers, driver's license numbers, etc., to include biometric

---

companies to notify persons affected by breaches involving their personal information, and in some cases to implement information security programs to protect the security, confidentiality, and integrity of data.").

[43] *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/29FJ-BC3H] ("All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identiable information.").

[44] *Id.* ('Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).').

[45] 2019 *Security Breach Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (July 26, 2019), http://www.ncsl.org/research/telecommunica tions-and-information-technology/2019-security-breach-legislation.aspx [https://perma.cc/795F-MFGC] ("At least 21 states in 2019 considered measures that would amend existing security breach laws.").

[46] *Id.* (discussing trends in legislation of new proposals in 21 states).

[47] *Id.* (discussing new legislation in New York: AB 2374 and SB 5575).

information such as finger prints.[48] The civil penalty for noncompliance also increased from ten dollars per instance of failed notification to twenty dollars per instance.[49] The second newly enacted amendment requires consumer credit reporting agencies to offer identity theft prevention and mitigation services in case of a breach.[50] In regards to notification, the current law does not have an explicit time limit, but states that disclosure should "be made in the most expedient time possible and without unreasonable delay"—leaving plenty of space for ambiguities.[51] Other states have similar pending legislation focused on expanding the definitions of personal information, shortening the timeframe for reporting, and requiring credit freezes for consumers, but currently New York and California generally have the most aggressive laws.[52]

Nevertheless, the data breach notification laws in the United States are still based on a "sectoral" approach on an aggregate level.[53] This means that data security regulations vary "on a sector-by-sector

---

[48] S. Assemb. 5575B, 2019–20 Reg. Sess. (N.Y. 2019) (discussing the inclusion of biometric information "such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity").

[49] *Id.* ("Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to twenty dollars per instance of failed notification, provided that the latter amount shall not exceed two hundred fifty thousand dollars.").

[50] S. Assemb. 2374, 2019–20 Reg. Sess. (N.Y. 2019) ("Upon a breach of the security of the system of a consumer credit reporting agency which includes any social security number, such agency shall offer to each consumer, whose information, including social security number, was breached or is reasonably believed to have been breached, reasonable identity theft prevention services and, if applicable, identify theft mitigation services for a period not to exceed five years at no cost to such consumers.").

[51] S. Assemb. 1387, 2019–20 Reg. Sess. (N.Y. 2019) ("Any person of business . . . shall disclose any breach of the security of the system within five days of the discovery or notification of the breach. . ."); N.Y. GEN. BUS. LAW § 899-aa (Consol. 2019) ("The disclosure shall be made in the most expedient time possible and without unreasonable delay. . . .").

[52] 2019 *Security Breach Legislation*, *supra* note 45 (discussing upcoming bills in 21 U.S. states for comparison).

[53] SOLOVE & SCHWARTZ, *supra* note 36, at 45–46 ("In contrast, the United States has generally relied on regulation of information use on a sector-by-sector basis.").

basis"; "[d]ifferent industries receive different regulation, and some contexts are not regulated at all."[54] In contrast, the European Union (EU) has taken an "omnibus" approach with a single law that protects "personal data across all industries" by adopting the General Data Protection Regulation (GDPR).[55] The GDPR has a broad material and territorial scope, applying to any "processing of personal data" within the EU.[56] A few provisions noticeably different than current U.S. data breach laws are: inclusion of "physical, physiological, genetic, [and] mental" data in personal information; a strict timeframe of 72 hours for breach notification; and a penalty of up twenty million Euros or four percent of a company's global turnover for noncompliance.[57] While the GDPR provisions are visbly stronger than their U.S. counterparts, the latest amendments in the aforementioned U.S. state laws likely represent an attempt to align with EU standards.

---

[54] *Id.* ("Sectoral: Regulates information on a sector-by-sector basis. Different industries receive different regulation, and some contexts are not regulated at all. Different statutes regulate the public and private sectors.").

[55] *Id.* at 45, 52 ("Omnibus: A comprehensive approach to protecting privacy that covers personal data across all industries and most contexts.").

[56] Art. 2, 3, General Data Protection Regulation, INTERSOFT CONSULTING, https://gdpr-info.eu [https://perma.cc/TQ34-B9V4; https://perma.cc/8FGB-4N9L] (last visited Oct.6, 2019) ("This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.") ("This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.").

[57] Art. 4, 33, 83, General Data Protection Regulation, INTERSOFT CONSULTING, https://gdpr-info.eu [https://perma.cc/8895-GXGH; https://perma.cc/V5RV-TBZG; https://perma.cc/S4ZG-PN2Y] (last visited Oct.6, 2019) ("In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent . . .") ("Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher . . .").

D. Conclusion and Predictions: What Happens from Here?[58]

As more and more transactions take place online, data security has become a primary concern for modern financial institutions. There is no doubt that data breach incidents are on the rise every year, and this upward trend would likely persist in the future. For data breach legislation in the United States, a shift from a sectoral approach to an omnibus approach—like that of the EU's GDPR—is definitely beneficial. While the upfront cost for implementing an omnibus approach would be higher, in the long run, the current patchwork sectoral process takes even more time and resources to accomplish. In addition, under the sectoral approach, the variance in state laws subjects citizens from different states to different levels of protection from data breach incidents, producing an unequal treatment for victims of such incidents. The ongoing process of amending state laws in data breach protection towards the GDPR direction is a move in the right direction, as pushing for stricter requirements on the state level would prepare the nation for a more unified framework that would more effectively protect consumers. The fact that many multinational corporations today have separate and additional data use policies for EU customers than for U.S. customers shows that stricter requirements and harsher penalties for noncompliance incentivize companies to handle user data more carefully. It is worth keeping up with the latest developments in the aforementioned state laws as their progress will be an important indicator for the future trend of data breach laws in this country.

Zhiyao Li[59]

---

[58] *See supra* Sections II, III (discussing the Capital One incident and the status of data breach laws in the US as well as EU).

[59] Student, Boston University School of Law (J.D. 2021).