UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 25 | Issue 1 Article 15

3-1-2021

# The Brick-and-Mortar Bank is Dead—COVID-19 Killed It: Analyzing the "New Normal" for Data Security in the Increasingly Digital Financial Services Industry

Anna-Nicole Cooke

# The Brick-and-Mortar Bank is Dead—COVID-19 Killed It: Analyzing the "New Normal" for Data Security in the Increasingly Digital Financial Services Industry

## I. INTRODUCTION

A rule of thumb is to strike while the iron is hot; for cybercriminals, that iron is a global pandemic.[1] The novel coronavirus dubbed "COVID-19" is an infectious disease that was first identified in Wuhan, China in December 2019.[2] In March 2020, the World Health Organization ("WHO") officially declared the COVID-19 disease a pandemic following rapid global transmission.[3] This pandemic brought the world to a screeching halt as governments frantically tried to "flatten the curve."[4] Indeed, COVID-19's effects permeated nearly every layer

1. *See* Ellen Sheng, *Cybercrime Ramps Up Amid Coronavirus Chaos, Costing Companies Billions*, CNBC, https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html [https://perma.cc/DRJ7-KKL5] (last updated July 29, 2020, 12:00 PM) (discussing the increase in the frequency and intensity of data breaches during the COVID-19 pandemic).

2. *See Frequently Asked Questions*, CTR. FOR DISEASE CONTROL, https://www.cdc.gov/coronavirus/2019-ncov/faq.html [https://perma.cc/Y7U2-94FC] (last updated Jan. 19, 2021) (stating that COVID-19 is a novel disease that was first discovered in Wuhan, China); *see also Coronavirus*, WORLD HEALTH ORG., https://www.who.int/health-topics/coronavirus#tab=tab_1 [https://perma.cc/9BBQ-N25P] (last visited Feb. 6, 2021) (discussing how COVID-19 quickly spreads among people through saliva or discharge from the nose).

3. *See, e.g.*, Mert Topcu & Omer Serkan Gulal, *The Impact of Covid-19 on Emerging Stock Markets*, 36 FIN. RES. LETTERS at 1, 1 (July 10, 2020) (stating that the pandemic was officially declared as such on March 11, 2020, having spread to 216 countries).

4. *See* Maria Nicola et al., *The Socio-Economic Implications of the Coronavirus Pandemic (COVID-19): A Review*, 78 INT'L J. SURGERY 185, 185 (2020) ("Social distancing, self-isolation and travel restrictions have lead to a reduced workforce across all economic sectors and caused many jobs to be lost. Schools have closed down, and the need for commodities and manufactured products has decreased. . . . The food sector is also facing increased demand due to panic-buying and stockpiling of food products."); Kim Parker et al., *Economic Fallout From COVID-19 Continues To Hit Lower-Income Americans the Hardest*, PEW RES. CTR. (Sept. 24, 2020), https://www.pewsocialtrends.org/2020/09/24/economic-fallout-from-covid-19-continues-to-hit-lower-income-americans-the-hardest/ [https://perma.cc/Y582-6VAD] (stating that the pandemic has caused many Americans to experience financial hardship); Brandon Specktor, *Coronavirus: What Is 'Flattening the Curve,' and Will It Work?* LIVE SCI. (Mar. 16, 2020), https://www.livescience.com/coronavirus-flatten-the-curve.html [https://perma.cc/NUE7-Z493] (explaining that in epidemiology, "flattening the curve" refers

of American society,[5] while the banking and finance sectors suffered an especially significant blow.[6] The pandemic delivered a plethora of shocks, including to economic supply and demand, as well as to digital markets.[7] This downturn has surpassed the turmoil of both the Great Depression and the 2008 financial crisis.[8] Global stock markets became alarmingly volatile.[9] The Dow Jones Industrial Average and the NASDAQ dramatically declined.[10] The bond market nearly broke down,[11] and consumer spending fell drastically.[12] Although the most

to slowing the spread of a virus so that there are enough hospital beds, doctors, and resources to treat infected patients).

5. *See* Nicola et al., *supra* note 4, at 185–90 (analyzing COVID-19's impact on different sectors of the economy, including, but not limited to: agriculture, oil, manufacturing, education, and finance).

6. *See id.* at 187 ("The decline in global stock markets has festered a volatile environment with critical liquidity levels.").

7. *See* Adam Triggs & Homi Kharas, *The Triple Economic Shock of COVID-19 and Priorities for an Emergency G-20 Leaders Meeting*, BROOKINGS INST. (Mar. 17, 2020), https://www.brookings.edu/blog/future-development/2020/03/17/the-triple-economic-shock-of-covid-19-and-priorities-for-an-emergency-g-20-leaders-meeting/ [https://perma.cc/DEN7-6Z83] (discussing how an emergency G-20 leaders' meeting was been called to address the financial shocks resulting from COVID-19); *see also* Sergej Epp, *The Great Digital Shock: Adapting to a New Normal in Cybersecurity*, PALOALTONETWORKS (Aug. 20, 2020), https://www.securityroundtable.org/the-great-digital-shock-adapting-to-a-new-normal-in-cybersecurity/ [https://perma.cc/ZE8J-AKJL] (analyzing how digitalization has helped cushion the economic fallout of COVID-19, and how the pandemic will accelerate the need for cybersecurity among businesses).

8. *See* Gita Gopinath, *The Great Lockdown: Worst Economic Downturn Since the Great Depression*, IMF: IMFBLOG (Apr. 14, 2020), https://blogs.imf.org/2020/04/14/the-great-lockdown-worst-economic-downturn-since-the-great-depression/ [https://perma.cc/RV5H-8CFY] ("[T]he Great Lockdown [is] the worst recession since the Great Depression, and far worse than the Global Financial Crisis.").

9. *See* Nicola et al., *supra* note 4, at 187 (analyzing the decline in global stock markets, and how these markets have fallen to critical liquidity levels).

10. *See id.* ("In addition to the disruption in the supply chain, the capital market sector has also been affected. In the US, the S&P 500, a stock market index that measures the stock performance of 500 large companies on the US stock exchange, the Dow Jones Industrial Average and the Nasdaq fell dramatically until the US government secured the Coronavirus Aid, Relief, and Economic Security (CARES) Act[.]").

11. *See* Jacob Manoukian, *COVID-19 Almost Broke the Bond Market. Then the Fed Stepped In.* JPMORGAN (Mar. 30, 2020), https://www.jpmorgan.com/securities/insights/covid-19-almost-broke-the-bond-market-then-the-fed-stepped-in [https://perma.cc/4PX6-ZVUE] (discussing how the Federal Reserve stepped in with unprecedented policy responses to resuscitate the bond market).

12. *See* Richard D. Harroch et al., *The Impact of the Coronavirus Crisis on Mergers and Acquisitions*, FORBES (Apr. 17, 2020, 6:00 AM), https://www.forbes.com/sites/allbusiness/2020/04/17/impact-of-coronavirus-crisis-on-mergers-and-acquisitions/#5403eba0200a [https://perma.cc/ZRD6-5FBB] (stating that COVID-19 has affected scores of businesses, workers, and consumers).

pressing concerns of the COVID-19 pandemic have been the sharp increase in cases, loss of lives, and economic shutdowns, the spike in data breaches and its insidious impact cannot be overlooked.[13]

COVID-19 and its subsequent expansion of work-from-home policies will have lasting implications on the data security of financial institutions.[14] The pandemic forced banks to adapt to a "new normal,"[15] which has entailed a shift away from the physical banking model.[16] This new normal has made digitalization the future of finance and banking in a post-pandemic world.[17] For example, financial institutions saw a decline in the use of cash and a surge in the popularity of contactless payments during the pandemic.[18] The American economy has undergone

13. *See* Sheng, *supra* note 1 (examining how cybercriminals have capitalized on the uncertainty caused by the pandemic to scam people and businesses).

14. *See* Richard Yao, *The Long-Lasting Impact of COVID-19 on Digital Payments*, MEDIUM (Aug. 20, 2020), https://medium.com/ipg-media-lab/the-long-lasting-impact-of-covid-19-on-digital-payments-40aa2bf4cb19 [https://perma.cc/H7AL-UKJQ] (predicting that the pandemic is the turning point for digital payment adoption); *see also* Amit Gautam, *How Will Long-Term Work-From-Home Impact Innovation, Collaboration and Mental Health?* FORBES (Dec. 14, 2020, 9:20 AM), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/how-will-long-term-work-from-home-impact-innovation-collaboration-and-mental-health/?sh=3c3caca32c33 [https://perma.cc/GQ4T-WJCF] (evaluating the pros and cons of a permanent remote workforce).

15. *See* Lisa Rowan, *How the Banking Experience Is Adapting to the COVID-19 'New Normal*,' FORBES (Sept. 3, 2020, 2:16 PM), https://www.forbes.com/sites/advisor/2020/09/03/how-the-banking-experience-is-adapting-to-the-covid-19-new-normal/#6099dee2efd0 [https://perma.cc/4E9V-FG7T] (scrutinizing the operational adjustments banks may have to make in a post-pandemic world).

16. *See* Allissa Kline, *Digital Banking: Once-Steady Shift Now Moving at Lightning Speed*, AM. BANKER (June 23, 2020, 9:30 PM), https://www.americanbanker.com/news/digital-banking-once-steady-shift-now-moving-at-lightning-speed [https://perma.cc/TQ9T-PJ2Y] ("What we're seeing is the *greatest acceleration* of digital banking in history[.]") (emphasis added) (referring to the increase in digital banking during the pandemic); *see also* Scott Baret et al., *COVID-19 Potential Implications for the Banking and Capital Markets Sector*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/economy/covid-19/banking-and-capital-markets-impact-covid-19.html [https://perma.cc/YN95-WZ79] (examining how banks may need to rely more on digital banking to bolster operational resilience throughout the pandemic).

17. *See* Jim Marous, *COVID-19 Accelerates Urgency for Digital Banking Transformation*, THE FIN. BRAND (June 18, 2020), https://thefinancialbrand.com/97453/covid-19-coronavirus-digital-innovation-transformation-trend-capgemini-amazon/ [https://perma.cc/UR4H-UB75] (analyzing how the increased rate of digitalization requires financial institutions to reevaluate their existing business models).

18. *See* Olivia Petter, *Coronavirus: Avoid Banknotes and Switch to Contactless Payments to Avoid Transmission, Suggests WHO*, THE INDEP. (Mar. 4, 2020, 12:18), https://www.independent.co.uk/life-style/health-and-families/coronavirus-news-banknotes-world-health-organisation-contactless-payment-a9374441.html [https://perma.cc/C8DZ-

an unplanned social experiment, courtesy of the work-from-home model.[19] Cybercriminals have capitalized on the economic turmoil and uncertainty.[20] As more institutions embrace digitalization in order to survive in the increasingly digital world, the consumer data they possess becomes more vulnerable to cyberattacks.[21] Therefore, it is time for financial institutions to perfect their data security measures, while urging lawmakers to reform legislation in light of these updates.[22] Improving data privacy legislation will increase consumer trust in financial institutions, safeguard consumers from additional data injury, and reduce the financial impact companies incur after a breach.[23]

---

8SXF] (discussing advice from the World Health Organization on using contactless payments to prevent the further spread of COVID-19); *see also* Stephanie Walden, *Banking After Covid-19: The Rise of Contactless Payments in the U.S.*, FORBES (June 12, 2020, 8:02 AM), https://www.forbes.com/advisor/banking/banking-after-covid-19-the-rise-of-contactless-payments-in-the-u-s/ [https://perma.cc/J56A-N66P] ("Overall usage of contactless payments in the country has risen 150% since March 2019.").

19. *See Cyber Crime – The Risks of Working from Home*, DELOITTE, https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html [https://perma.cc/5MU2-83D8] (last visited Feb. 6, 2021) (discussing how COVID-19 has changed criminal activity, with cybercriminals increasingly targeting people using technology at home instead of at the office).

20. *See id.* ("Cyber criminals are switching tactics and exploiting COVID-19-related fears among the population. As a result, working from home is becoming a gateway to new forms of data theft.").

21. *See* RISK BASED SEC., INC., *2020 Q1 Data Breach Report QuickView* (2020), https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q1%20Data%20Breach%20QuickView%20Report.pdf?hsCtaTracking=5d936f78-de69-45a4-9ba5-03c2e9f20952%7C617588df-ee05-4a00-bbb1-191d6888f519 [https://perma.cc/YRK3-FJY5] ("[I]ncreased digitalization mak[es] data more vulnerable than ever.").

22. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/38S3-U5HB] ("The U.S. Congress should join other advanced economies in their approach to data protection by creating a single comprehensive data-protection framework. Meaningful federal laws and regulations should seek to resolve the differences among the existing federal and state legal rights and responsibilities. This would not only simplify compliance for U.S. companies, but would also strengthen and bring the United States in line with emerging data-protection norms.").

23. *See, e.g.*, *Data Breach Cost Part One: Risks, Costs and Mitigation Strategies for Data Breaches*, ZURICH 2–6, http://cdn.theatlantic.com/static/front/docs/sponsored/zurich-risk/DataBreachCost_Zurich.pdf [https://perma.cc/V6AV-F4EA] (last visited Dec. 29, 2020) (breaking down the costs a company may incur after a data breach); Einat Weiss, *Data Privacy Rules Are Changing. How Can Marketers Keep Up?* HARVARD BUS. REV. (Aug. 27, 2020), https://hbr.org/2020/08/data-privacy-rules-are-changing-how-can-marketers-keep-up [https://perma.cc/TV2Q-77NN] ("[The European Union's General Data Protection Regulation and the California Consumer Privacy Act] give consumers more awareness and control over exactly what personal information is collected, how it is sold, and how its security is ensured."); O'Connor, *supra* note 22 (recommending that the United States enact a comprehensive data protection law in order to better protect the data of U.S. citizens).

This Note proceeds in seven parts. Part II explores the background on data security and the data security risks faced by financial institutions before the pandemic.[24] Part III examines current data protection laws pertaining to consumer financial data.[25] Part IV assesses the present impact of COVID-19 on the financial services industry, including the expansion of telework and the proliferation of mobile banking.[26] Part V considers the future impact of COVID-19, including new threats to consumer data arising from the shift to a remote workforce.[27] Part VI recommends potential actions financial institutions can take to mitigate the risk of consumer data injury in the increasingly digital financial world.[28] Part VII summarizes the argument and concludes this Note.[29]

## II. BACKGROUND ON DATA SECURITY IN THE FINANCIAL SERVICES INDUSTRY

### *A. Data Breaches and Their Far-Reaching Impact*

A data breach is an unauthorized entry into a database which allows hackers access to consumer information.[30] Breaches have the potential to compromise highly sensitive personal information including: Social Security numbers, credit card numbers, banking information, and passwords.[31] System vulnerabilities allow hackers to invade these databases.[32] The standard assumption is that these hackers are motivated

24. *See infra* Part II.

25. *See infra* Part III.

26. *See infra* Part IV.

27. *See infra* Part V.

28. *See infra* Part VI.

29. *See infra* Part VII.

30. *See* Nicole Martin, *What Is a Data Breach?* FORBES (Feb. 25, 2019, 12:27 PM), https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#70dd67ba14bb [https://perma.cc/3MJW-VXSV] (defining the term data breach and examining the biggest data breach cases across different industries).

31. *See id.* (explaining that these sensitive sources of information are exploited by cybercriminals for identity theft and other forms of fraud).

32. *See 4 Types of Data Breaches You Need to Know*, INTERNOS (Oct. 2, 2019), https://www.gointernos.com/the-4-types-of-data-breaches-you-need-to-know/ [https://perma.cc/3FBB-9PVN] (discussing the four major types of data breaches: malware, phishing, ransomware, and denial of service).

by financial gain.[33] While evading the risk of prison or federal prosecution, "smart" hackers can make thousands, or even millions, of dollars.[34] Targeted criminal activity is the source of numerous breaches.[35] However, the majority of data breaches are actually caused by human or system error.[36] Human error occurs when employees access data without authorization, handle information or hardware improperly, or violate federal or industry regulations.[37] System error happens when a large amount of data is inadvertently transferred from one system to another.[38] Regardless of the type of error, breaches can have devastating impacts,[39] especially if they are not discovered quickly.[40]

Data breaches may go undetected for weeks and even months,[41] despite the fact that a data breach occurs nearly everyday.[42] In the financial services industry, it takes an average of 233 days to identify and contain a breach.[43] In the meantime, stolen personal information can

33. *See* Joseph F. Yenouskas & Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, A.B.A. (July 17, 2018), https://www.americanbar.org/groups/business_law/publications/blt/2018/07/data-breach/ [https://perma.cc/5BJ4-NFBK] ("[E]xisting case law is largely based on the assumption that hackers steal PII [or personally identifiable information] for financial gain, even though hackers are increasingly motivated by non-commercial ends, such as activism, blackmail, or espionage.").

34. *See* James Lewis, *Economic Impact of Cybercrime: No Slowing Down*, MCAFEE 4 (Feb. 2018), https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf [https://perma.cc/FW2S-9SW2] ("A smart cybercriminal can make hundreds of thousands, even millions of dollars *with almost no chance* of arrest or jail.") (emphasis added).

35. *See* Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1174 (2014) ("[T]wo-thirds of data breaches are actually caused by human or system error.").

36. *See id.*

37. *See id.* (explaining the various ways in which human error can lead to a data breach).

38. *See id.* (explaining the various ways in which system error can lead to a data breach).

39. *See id.* (discussing huge data breaches that occurred within Target, Home Depot, and JP Morgan Chase).

40. *See* Aimee O'Driscoll, *30+ Data Breach Statistics and Facts*, COMPARITECH (Dec. 10, 2020), https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/ [https://perma.cc/4L2V-NWJQ] (revealing that data breach disclosure reports may be inaccurate given that many breaches go undetected).

41. *See* PONEMON INST., *2020 Cost of a Data Breach Report*, 54 (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf [https://perma.cc/6BNC-7BJF] (analyzing data breaches that occurred between August 2019 and April 2020, showing that it takes approximately 280 days (depending on industry) to identify and contain a breach).

42. *See* Peters, *supra* note 35, at 1172 ("Hardly a day passes without a data breach, and many remain undiscovered for months or even years.").

43. PONEMON INST., *supra* note 41, at 54.

travel to black markets or the dark web.[44] Moreover, data breaches do not affect all industries equally: the financial services industry is disproportionately impacted.[45] In fact, a spokesperson for the Securities and Exchange Commission declared cyberattacks on financial institutions to be "the most pressing issue in corporate governance today."[46] Compared to other industries, banks have more to lose when a breach occurs.[47]

Data breaches expose banks to financial, reputational, and legal risks.[48] It is becoming increasingly common for banks to pay millions of dollars in settlements with regulators and then implement new security protocols after a breach.[49] Incidents that compromise consumers'

44. *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 349 (2019) (discussing the existence of a black market for personal consumer financial information); Doug Shadel & Neil Wertheimer, *Is My Identity on the Dark Web?* AARP (Sept. 4, 2018), https://www.aarp.org/money/scams-fraud/info-2018/what-is-the-dark-web.html [https://perma.cc/B9YS-WE5D] (detailing the takedown of a deep web website, AlphaBay, which had listings for 4,488 stolen identification numbers and 28,800 stolen credit card numbers); Darren Guccione, *What is the Dark Web? How to Access it and What You'll Find*, CSO (Nov. 18, 2020, 3:00 AM), https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html [https://perma.cc/CQ7H-7G83] (stating that the dark web is a part of the internet that is invisible to search engines where "[y]ou can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers").

45. *See* Kesan & Hayes, *supra* note 44, at 303–04 ("[T]he finance and insurance industries had the highest number of total [data breach] incidents at 5,512.").

46. *See* Robert J. Jackson, Jr., *Corporate Governance: On the Front Lines of America's Cyber War* (Mar. 15, 2018), https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15 [https://perma.cc/7J39-56K8] (discussing how the increasing digital transformation in the United States has given rise to a growing cyber threat).

47. *See* Dan Ennis, *Banks Have More to Lose from Data Breaches Than Other Companies*, BANKING DIVE (Sept. 4, 2019), https://www.bankingdive.com/news/bank-data-breach-timely-direct-response-experian/562209/ [https://perma.cc/NVJ2-QKK2] (reporting that survey evidence indicates that financial institutions are at a greater risk to lose their reputation and consumers when a breach occurs in comparison to other industries).

48. *See* Christina Parajon Skinner, *Bank Disclosures of Cyber Exposure*, 105 IOWA L. REV. 239, 249 (2019) (explaining how banks may be required by federal securities law to publicly disclose operational risks such as data breaches); *see also* Ennis, *supra* note 47 (examining how banks' consumer base and reputation are on the line when a data breach occurs).

49. *See Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FED. TRADE COMM'N. (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/N4HQ-TYBX] [hereinafter *Equifax to Pay $575 Million*] (examining the details of Equifax's proposed $575 million settlement agreement with the Federal Trade Commission, Consumer Financial Protection Bureau, and U.S. states and territories as a result of Equifax's 2017 data breach); *see also* Kevin Wack, *Capital One to Pay $80M in Connection with Massive Data Breach*, AM. BANKER (Aug. 6,

personal information are the most costly, and most common, type of breach.[50] Further, the reputation of the bank is on the line when it experiences a data breach, regardless of the severity or scope of the breach.[51] It is well documented that data breaches do irreparable harm to consumer trust.[52] Following Equifax's 2017 breach, consumer data showed the company to be the least trusted of the three major credit reporting agencies.[53] In fact, lost business profits resulting from the lack of consumer trust—like customer turnover and efforts directed at acquiring new customers—account for approximately 40% of the average total cost of a breach (a whopping $1.52 million).[54]

---

2020, 12:30 PM), https://www.americanbanker.com/news/capital-one-to-pay-80m-in-connection-with-massive-data-breach [https://perma.cc/Y5NJ-CRTR] (disclosing details of Capital One's $80 million settlement with the Office of the Comptroller of the Currency following the bank's 2019 data breach, including the requirement that Capital One develop new cybersecurity action plans).

50. *See* PONEMON INST., *supra* note 39, at 8 ("Customers' personally identifiable information (PII) was the most frequently compromised type of record, and the costliest, in the data breaches studied.").

51. *See, e.g.*, *Consumer Intelligence Series: Protect.me*, PWC at 3 (2017), https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf [https://perma.cc/9Y5U-RPM9] [hereinafter *Consumer Intelligence Series*] (reporting that 85% of consumers will not do business with a company that has dubious security practices); *see also 81% of Consumers Would Stop Engaging with a Brand Online after a Data Breach, Reports Ping Identity*, BUS. WIRE (Oct. 22, 2019, 8:00 AM), https://www.businesswire.com/news/home/20191022005072/en/81-of-Consumers-Would-Stop-Engaging-with-a-Brand-Online-After-a-Data-Breach-Reports-Ping-Identity [https://perma.cc/J7VA-ZZ9] [hereinafter *81% Would Stop Engaging after a Data Breach*] (reporting that 81% of survey respondents would stop engaging in business with a company that suffered a data breach); Ennis, *supra* note 47 ("[F]inancial services companies have more to lose — both in reputation and customer base — than do other businesses.").

52. *See, e.g.*, *Consumer Intelligence Series, supra* note 51, at 3 (providing statistics on how consumers expect regulators and companies to safeguard their data); *81% Would Stop Engaging after a Data Breach*, *supra* note 51 (using statistical data to show that consumers may abandon a brand if their personal data was not protected by the company); Ennis, *supra* note 47 ("[Sixty-six percent] of people surveyed said they would stop doing business with a company that had a slow or ineffective response to a data breach and would switch to a competitor. And 45% said they would tell their family and friends to stop doing business with the company.").

53. *See* Sabrina Karl, *Consumer Trust in Equifax Sinks after Data Breach*, CREDITCARDS.COM (Mar. 26, 2018), https://www.creditcards.com/credit-card-news/equifax-consumer-trust-after-breach/ [https://perma.cc/LS3S-TRVA] (reporting that, after the Equifax breach, 28% of surveyed consumers did not trust Experian, 27% did not trust TransUnion, and a whopping 40% of consumers did not trust Equifax).

54. PONEMON INST., *supra* note 39, at 10.

Another painful repercussion on a bank's reputation stems from attacks on its credibility.[55] A breach may lead to doubts of the breached bank's ability to protect its depositors.[56] This mistrust can produce a "trickle-up" panic effect, in which panic amongst depositors triggers a panic amongst lenders.[57] A breach can halt the "operational resilience" of a bank, damaging its ability to transfer credit or facilitate payments.[58] The inability of a bank to function properly could stall economic activity, making lenders anxious.[59] The activity of worried lenders—who doubt the resiliency of the bank—might result in higher margins on the bank's collateral and cause a drop in the value of its assets.[60]

On the legal side, breaches expose banks to potential class action lawsuits from affected customers.[61] The degree of data protection varies from state-to-state, as do the penalties.[62] Regardless, each state, at the

55. *See* Skinner, *supra* note 48, at 272 ("The public has a strong interest in the uninterrupted provision of the critical economic services that these big banks provide—payments, credit intermediation, and the provision of demand-deposit services. A cyberattack could threaten any or all of these functions at once.").

56. *See id.* ("An attack directed to a bank's infrastructure could, for instance, halt its ability to facilitate payments; an attack could also constrict the transfer of credit between financial institutions, or from banks to the real economy—any of these scenarios could bring real economic activity to a crawl or total halt. A cyberattack . . . could also be viewed by markets as a serious reputational event, which could incite depositor panic.").

57. *See id.* at 272 (discussing how stalled economic activity could contribute to serious reputational harm to a bank).

58. *See id.* ("A bank's operational resilience is a public good, too. The public has a strong interest in the uninterrupted provision of the critical economic services that these big banks provide—payments, credit intermediation, and the provision of demand-deposit services. A cyberattack could threaten any or all of these functions at once.").

59. *Id.*

60. *Id.*; *see* Christina Parajon Skinner, *Regulating Nonbanks: A Plan for SIFI Lite*, 105 GEO. L.J. 1379, 1421 (2017) ("A technological event (like a cyberattack or systems glitch or failure) also implicates run-risk insofar as the market could perceive an operational event as a reputational event, inciting panic. And operational events could lead to counterparty losses to the extent they prompt demands for higher margins on collateral (or the calling in of callable assets).").

61. *See* Yenouskas & Swank, *supra* note 33 (examining how data breaches have led to a plethora of class action lawsuits).

62. *See* Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, INT'L ASS'N OF PRIV. PROS. (June 8, 2020), https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/ [https://perma.cc/95WN-WSSB] (stating that California goes further in its data protection laws than other states by offering a private right of action to injured consumers); *see also* THE DEFINITIVE GUIDE TO U.S. STATE DATA BREACH LAWS, DIGIT. GUARDIAN 1, 1 (2018), https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf [https://perma.cc/7SLW-5P8Z] (reporting that many states impose civil penalties on companies that experience a breach).

minimum, has its own consumer notification requirements in the event of a data breach.[63] Thus, the burdens of a breach are compounded when a bank has to investigate the different state laws pertaining to affected customers to determine the legal guidelines for proper consumer notification.[64] That is, of course, assuming that a bank chooses to notify its consumers of the breach.[65]

The harm suffered from a breach extends far beyond the breached entity—it also affects the breached subjects.[66] The effects of a data breach encompass both tangible and psychological harms for its victims.[67] For consumers, financial injuries are frequently the most visible harms suffered as a result of a data breach.[68] Data harms have led to consumers losing their homes, filing for bankruptcy, having their utilities cut off, and incurring legal fees to recover damages resulting

63. *See* Ieuan Jolly, *Data Protection in the United States: Overview*, WESTLAW (database current June 8, 2020) (providing a high-level overview of federal and state data protection laws).

64. *See* Peters, *supra* note 35, at 1174–75 (explaining that state laws differ in its notification requirements and that it can be extremely burdensome for banks to comply with every state law pertaining to its breached consumers); *see generally* Jolly, *supra* note 63 (discussing the inconsistency of state laws regulating personal data collection, and how federal and state laws often "overlap, dovetail, and contradict one another").

65. *See 10,000 Breaches Later: Top Five Financial, Credit and Banking Data Breaches*, IDENTITY THEFT RES. CTR. (Nov. 12, 2019), https://www.idtheftcenter.org/10000-breaches-later-top-five-financial-credit-and-banking-data-breaches/ [https://perma.cc/L4E4-CGTD] (stating that JP Morgan Chase did not send out notification letters to scores of customers affected by its 2014 breach, which exposed personal information of seventy-six million households and seven million businesses). *But see* Kevin Wack, *Bank Regulators Mull Stricter Rules for Reporting of Data Breaches*, AM. BANKER (Dec. 14, 2020, 3:09 PM), https://www.americanbanker.com/news/bank-regulators-mull-stricter-rules-for-reporting-of-data-breaches [https://perma.cc/7YSL-DBMW] (discussing a potential push for new rulemaking by federal banking agencies, which would require banks to promptly report cyber security intrusions to their regulators).

66. *See* Max Meglio, Note, *Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation*, 61 B.C. L. REV. 1223, 1227 (2020) ("Data breaches create substantial costs that are borne by data subjects, the breached entity, and other third-parties.").

67. *See* Kesan & Hayes, *supra* note 44, at 347 (discussing how a data breach can encroach upon a consumer's autonomy).

68. *See id.* at 303 (discussing how data breaches are most commonly viewed in light of their financial impact); *see also* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 755–56 (2016) ("Requiring harm to be visceral and vested has severely restricted the recognition of data-breach harms, which rarely have these qualities. Data-breach harms are not easy to see, at least not in any physical way. They are not tangible like broken limbs and destroyed property. Instead, the harm is intangible.").

from a breach.[69] However, the impact of a breach cuts even deeper—it also injures a person's autonomy.[70] Victims can experience fear, anxiety, and stress over data breaches.[71] These psychological consequences may also have physical repercussions such as disturbances in sleep habits, trouble concentrating, aches, pains, headaches, and cramps.[72] Data breaches have even driven victims to suicide.[73]

Data breaches are also a huge drain on the global economy.[74] Richer countries are more affected by the costs associated with cybercrime.[75] The United States suffers the highest financial costs for data breaches.[76] On average, a U.S. bank suffers a loss of $3.86 million per data breach.[77] Due to the shift to remote work caused by COVID-19, the average total cost of a data breach in the United States is expected to increase to $4 million in 2021 given the growing number of human and digital targets.[78] Globally, the costs associated with cybercrime are

69. *See* Solove & Citron, *supra* note 68, at 756–57 (discussing ways in which a data breach can lead to financial ruin for consumers).

70. *See* Kesan & Hayes, *supra* note 44, at 347 (discussing an approach to digital harm which emphasizes the impact a breach has on a person's autonomy).

71. *See* Kesan & Hayes, *supra* note 44, at 336–37 ("[D]ata breaches offend social order. Society recognizes that theft is wrong. But theft is about things, and data breaches are often about people. The injury is harder to observe. Injuries caused by data breaches are often more psychological in nature, like apprehension of future injuries.").

72. *See* Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA TODAY, https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/ [https://perma.cc/35JF-NTMF] (last updated Feb. 24, 2020, 9:18 AM) (discussing the psychological harms that data injury victims face in the aftermath of a data breach).

73. *See, e.g.*, *id.* (revealing that some injured consumers committed suicide in the fallout of the Ashley Madison data breach); *see also* Laurie Seagall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN BUS. (Sept. 8, 2015, 7:10 PM), https://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/ (discussing the case of a pastor who committed suicide six days after hackers exposed the names of millions of consumers who used the Ashley Madison website, and how the pastor mentioned Ashley Madison in his suicide note).

74. *See* PONEMON INST., *supra* note 41, at 5–15 (breaking down the high costs of data breaches across the world, with the average total cost of a breach amounting to $3.86 million).

75. *See* Lewis, *supra* note 34, at 7 (reporting that the costs of cybercrime are unevenly distributed across the globe, with some countries affected more than others).

76. PONEMON INST., *supra* note 41, at 5.

77. *Id.*

78. *See id.* at 9 (reporting that a remote workforce will increase the cost of a data breach from $3.86 million to $4 million); *see also* Steve Morgan, *Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021*, CYBERCRIME MAG. (Dec. 7, 2018), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [https://perma.cc/5FV3-MWT4] (discussing how there will be more digital targets due to an

expected to rise to $6 trillion annually in 2021.[79] Cybercrime ultimately is a major threat to domestic and global economies because its ramifications touch everyone.[80]

### *B. How Prevalent Are Data Breaches?*

Cyberattacks are the fastest growing crime in the United States.[81] It is unlikely the rate of these attacks will decline given the growing number of consumers with "digital-first, branch second approach."[82] Indeed, the allure of digital banking has led the majority of consumers to prefer a digital relationship with their bank.[83] With constant access to their accounts, consumers often find online banking more convenient than having to visit a brick-and-mortar location.[84] Paying bills online is not only faster, but it also allows for recurring payments so consumers do not risk a penalty due to a forgotten bill.[85] Certain advantages incentivize

---

increase in wearable digital devices like smart watches, fitness monitors, and body-worn cameras).

79. *See* Morgan, *supra* note 78 (discussing the increase in global cybercrime costs to $6 trillion in 2021, which is double the total global cost of $3 trillion in 2015).

80. *See* Lewis, *supra* note 34, at 4 ("Where cybercrime is the undisputed leader, however, is in its ability to make hundreds of millions of people victims. . . . Cybercrime is front-page news because it touches everyone.").

81. *See* Morgan, *supra* note 78 (reporting that cybercrime costs are expected to increase in 2021).

82. *See* Brian Acton, *How Millennials Are Changing Banking*, POLICYGENIUS (Sept. 5, 2019), https://www.policygenius.com/blog/how-millennials-are-changing-banking/ [https://perma.cc/679M-JLF6] (examining the growing demand for digital banking platforms among millennials).

83. *See* Daniela Yu & Jon Hughes, *Struggle for Banks: Migrating Customers to Digital*, GALLUP (Oct. 27, 2016), https://news.gallup.com/businessjournal/196778/struggle-banks-migrating-customers-digital.aspx?utm_source=link_wwwv9&utm_campaign=item_237695&utm_medium=copy [https://perma.cc/LZT4-KP5B] (discussing how 56% of surveyed consumer bankers prefer using digital channels).

84. *See* Liz Knueven, *Online Banking Isn't Just for Millennials Anymore—it's Quickly Becoming the Norm*, BUS. INSIDER (Nov. 14, 2019, 2:13 PM), https://www.businessinsider.com/personal-finance/online-banking-gaining-popularity-united-states [https://perma.cc/BJ34-VP55] (examining how increasing numbers of millennials and Generation Z are using digital banking in comparison to baby boomers).

85. *See* Joe Young, *The Pros and Cons of Online Banking*, NASDAQ (Sept. 3, 2014, 8:39 AM), https://www.nasdaq.com/articles/pros-and-cons-online-banking-2014-09-03 [https://perma.cc/W47J-6GCT] (exploring how the advantages of online banking, such as automation and locational convenience, outweigh its disadvantages).

banks to foster this growing digitalization.[86] For instance, with less overhead costs for operating a digital platform, banks can offer higher interest rates on checking and savings accounts in addition to lower fees.[87] However, this digitalization puts consumer data at greater risk for cyberattacks.[88]

The increase in cyberattacks has led to rising costs in cybersecurity protection for banks.[89] The financial services sector spends three times the amount on cybersecurity safeguards compared to other industries.[90] Regulators agree that data breaches pose a systemic risk to a bank's operational resilience.[91] As a result, banks typically have safeguards in place including encryption, multifactor authentication, and biometric identity verification.[92] However, these measures are not

86. *See* Knueven, *supra* note 84 (discussing the advantages for banks opting for online platforms as opposed to brick-and-mortar locations, including, but not limited to: lower fees, higher interest rates, and convenience).

87. *See id.* ("While brick-and-mortar banks have to spend money to keep their branches open, online banks don't have that overhead. . . . [t]his is why online banks like Ally can offer financial products with big returns like high-yield savings accounts — compare Ally's variable APY of about 1.7% to 2.2% to traditional banks' .01% to .1% — and why *the bank branch down the street can't match that rate*.") (emphasis added).

88. *See* Jim Boehm et al., *Safeguarding Against Cyberattack in an Increasingly Digital World*, MCKINSEY (June 30, 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/safeguarding-against-cyberattack-in-an-increasingly-digital-world [https://perma.cc/ZXS2-VB2B] (discussing how the increasingly digitalized and automated world has made the threat of a data breach even more widespread).

89. *See* Michael McGinn, *Cost of Cybercrime Continues to Rise for Financial Services Firms, According to Report from Accenture and Ponemon Institute*, ACCENTURE (July 16, 2019), https://newsroom.accenture.com/news/cost-of-cybercrime-continues-to-rise-for-financial-services-firms-according-to-report-from-accenture-and-ponemon-institute.htm [https://perma.cc/7ZA4-XDRR] ("The cost to address and contain cyberattacks is greater for financial services firms than for companies in any other industry and the containment costs continue to inch upwards[.]").

90. *See* Lewis, *supra* note 34, at 9 ("Cybercrime imposes a heavy cost on financial institutions as they struggle to combat fraud and outright theft. One report says that banks spend three times as much on cybersecurity as non-financial institutions and there is agreement among bank regulators around the work that cybercrime poses a 'systematic' risk to financial stability.").

91. *Id.*

92. *See* Meredith E. Bock, Note, *Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act*, 24 N.C. BANKING INST. 309, 309 (2020) (stating that banks have incorporated biometrics into their security systems); *see also Business Data Security Guide (Measures, Risks & Precautions)*, SPIRION (Nov. 13, 2020), https://www.spirion.com/blog/business-data-security/ [https://perma.cc/5E5E-6BLN] (examining various data security measures businesses can take to mitigate the threat of a breach).

foolproof, especially when institutions neglect to patch vulnerabilities.[93] Such neglect has led to two of the most significant breaches: Capital One and Equifax.[94]

Capital One is the United States' fifth-largest consumer bank and the eighth-largest bank overall.[95] On July 19, 2019, it discovered that a breach compromised the personal information of approximately a hundred million Americans and six million Canadians.[96] The Office of the Comptroller of the Currency ("OCC"), the bank's federal regulator, said the breach was linked to problems with Capital One's cloud migration plan.[97] While the breach occurred in 2019, vulnerabilities within the bank's cloud migration plan dated back to 2015.[98] Within those four years, Capital One not only failed to implement network security controls, but its internal audits also failed to identify the weaknesses in its cloud operating systems.[99]

Following the breach, Capital One faced steep regulatory fines, was subject to several class-action lawsuits, and its stock plunged.[100]

93. *See Equifax to Pay $575 Million*, *supra* note 49 (mentioning that Equifax had been forewarned about the fatal security error that led to the company's 2017 breach); Wack, *supra* note 49 (discussing how problems with Capital One's cloud migration plan dated back to 2015, and Capital One's failure to remedy those problems contributed to the fateful 2019 breach).

94. *See Equifax to Pay $575 Million*, *supra* note 49 (discussing the details of Equifax's $575–$700 million settlement); *see also* Wack, *supra* note 49 ("Capital One Financial has reached settlements . . . in connection with a 2019 hacking incident that resulted in a massive compromise of customer data.").

95. *Our Company*, CAPITAL ONE, https://www.capitalone.com/about/corporate-information/our-company/ [https://perma.cc/HJ77-WEN7] (last visited Sept. 22, 2020).

96. *See Frequently Asked Questions*, CAPITAL ONE (Sept. 23, 2019, 4:15 PM), https://www.capitalone.com/facts2019/2/ [https://perma.cc/Q3SM-VA2F] (stating that Capital One discovered on July 19, 2019 that hackers had gained unauthorized access and obtained personal information about Capital One customers and applicants who had applied to become Capital One credit card customers); *see also* Wack, *supra* note 49 ("The hack compromised personal data on roughly 100 million Americans, and approximately 6 million Canadians, who either have a Capital One credit card or have applied for one. Capital One has said that roughly 140,000 Social Security numbers were exposed, as were 80,000 bank account numbers.").

97. Wack, *supra* note 49.

98. *Id.*

99. *Id.*

100. *See* Trefis Team & Great Speculations, *How Could the Recent Data Breach Affect Capital One's Stock?*, FORBES (Sept. 11, 2019, 9:15 AM), https://www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock/#42ab79c137b7 [https://perma.cc/WE4T-4HZK] (reporting that Capital One's stock has fallen from $100 per share to $85 per share after its 2019 breach, in addition to legal ramifications and penalties from its regulators).

Capital One notified all affected customers by mail and offered them two years of free credit monitoring.[101] As required by its settlement, Capital One agreed to develop and implement additional cybersecurity protocols.[102] The protocols included (1) appointing a compliance committee charged with sending periodic updates to the OCC, (2) proposing a "Comprehensive Action Plan" detailing its remedial actions, and (3) improving its cloud migration plan.[103]

Longstanding neglect also led the credit-reporting agency Equifax to suffer a massive data breach.[104] Despite being alerted of a critical security vulnerability in March 2017, Equifax's 225-person cybersecurity team failed to patch the network,[105] and by July 2017, it was too late.[106] Hackers invaded the vulnerable database and gained access to Equifax's network, compromising the personal data of 147 million consumers in the United States.[107] Unfortunately, the errors did not stop there.[108] After the breach, Equifax accidentally directed users to

---

101. *Frequently Asked Questions*, *supra* note 96.

102. Wack, *supra* note 49.

103. *See OCC Fines Capital One $80 Million for Cloud Security Violations Related to Cyber Breach*, WILLKIE COMPLIANCE (Aug. 7, 2020), https://complianceconcourse.willkie.com/articles/news-alerts-2020-08-august-20200807-occ-fines-capital-one-80-million [https://perma.cc/D3M3-LSV3] (discussing how Capital One will have to appoint a Compliance Committee to submit updates to the OCC, develop a "Comprehensive Action Plan" detailing remedial actions, and submit risk assessment, audit, and oversight management reports to the OCC).

104. *See Equifax to Pay $575 Million*, *supra* note 49 (reporting that Capital One's "failure to take reasonable steps to secure its network led to a data breach in 2017 that affected approximately 147 million people.").

105. *See* Sarah Buhr, *Former Equifax CEO Says Breach Boiled Down to One Person Not Doing Their Job*, TECHCRUNCH (Oct. 3, 2017, 3:24 PM), https://techcrunch.com/2017/10/03/former-equifax-ceo-says-breach-boiled-down-to-one-person-not-doing-their-job/ [https://perma.cc/8LH2-GK37] (examining the details of the Capital One data breach and the difficulty in holding its employees accountable for the breach).

106. *See Equifax to Pay $575 Million*, *supra* note 49 (discussing how Equifax finally discovered its critical security error in July 2017, where it discovered that cybercriminals had had access to consumers' personally identifiable information for months).

107. *See Equifax to Pay $575 Million*, *supra* note 49 ("[H]ackers stole at least 147 million names and dates of birth, 145.5 million Social Security numbers, and 209,000 payment card numbers and expiration dates.").

108. *See* Selena Larson, *Equifax Tweets Fake Phishing Site to Concerned Customers*, CNN BUS. (Sept. 20, 2020, 4:17 PM), https://money.cnn.com/2017/09/20/technology/business/equifax-fake-site-twitter-phishing/index.html [https://perma.cc/6K39-CFZ5] (examining how Equifax addressed customer service complaints and concerns relating to its 2017 breach, but in doing so, directed

a phishing site and retracted public statements multiple times—including a statement that previously said consumers could not sue the company.[109] Consumer trust plummeted.[110] Over half of Equifax consumers in one survey indicated that they no longer trusted the agency with their personal information.[111] The breach resulted in consumers experiencing anxiety, anger, and fear of data insecurity.[112]

As a result of this breach, Equifax paid out $575 million and potentially up to $700 million in its settlement with the Federal Trade Commission ("FTC"), Consumer Financial Protection Bureau ("CFPB"), and every U.S. state and territory.[113] In an attempt to address this, Equifax laid out a three-year plan to regain consumer trust.[114] With $200 million invested in the plan, Equifax claimed that consumer trust would be restored by 2020.[115] Survey data supports this claim, showing that consumers are slowly regaining trust in Equifax.[116] Public opinion of

customers to the phishing site "securityequifax2017.com" instead of the legitimate site "equifaxsecurity2017.com").

109. *See id.* (discussing how Equifax tweeted links to a fake website to customers asking for help and more information about the company's 2017 breach); *see also* Buhr, *supra* note 102 (stating that, although Equifax had a 225-person cybersecurity team, no one on that team realized that "a patch for that vulnerability [that caused the breach] had been available for months before the breach occurred."); Geraldine Strawbridge, *5 Ways to Identify a Phishing Website*, METACOMPLIANCE (July 2, 2018), https://www.metacompliance.com/blog/5-ways-to-identify-a-phishing-website/ [https://www.metacompliance.com/blog/5-ways-to-identify-a-phishing-website/] ("Phishing continues to prove one of the most successful and effective ways for cybercriminals to defraud us and steal our personal and financial information.").

110. *See* Karl, *supra* note 53 ("Consumer trust in Equifax sank after its 2017 data breach.").

111. *See id.* (stating that Equifax became the least trusted of the three major credit reporting bureaus following the 2017 breach).

112. *See Identity Theft Resource Center Sees Major Consumer Impacts One Year After the Equifax Breach*, IDENTITY THEFT RES. CTR. (Sept. 10, 2018), https://www.idtheftcenter.org/identity-theft-resource-center-the-aftermath-equifax-one-year-later/ [https://perma.cc/3A7K-N53W] (discussing how many victims of the Equifax breach felt adverse or negative emotions following the incident, including feeling anxious, violated and/or unsafe).

113. *Equifax to Pay $575 Million*, *supra* note 49.

114. *See* Alfred Ng, *Equifax Has a Plan to Win Your Trust Back. It'll Take Three Years.* CNET (Aug. 10, 2018, 5:00 AM), https://www.cnet.com/news/equifax-has-a-plan-to-win-your-trust-back-itll-take-three-years/ [https://perma.cc/7952-UH9K] (examining Equifax's new chief information security officer's plan to win back customers following the 2017 breach).

115. *Id.*

116. *See* David Lord, *Equifax Somehow Managed to Regain Public Trust*, MARKETWATCH (Nov. 7, 2018, 9:55 PM), https://www.marketwatch.com/story/equifax-somehow-managed-to-regain-public-trust-2018-11-07 [https://perma.cc/BD8U-DF7Z] (stating that public opinion of Equifax is almost at the same spot, -2, as it was before the 2017 data breach occurred).

Equifax is now at the same place it was before the breach happened.[117] The Capital One and Equifax data breaches ultimately exemplify the far-reaching impacts a breach can have on the financial services industry.[118] Unfortunately, the inadequacy of federal and state laws regulating personal consumer data collection exacerbates the frequency and impact of a breach.[119]

## III. DATA PROTECTION LAWS REGULATING CONSUMER FINANCIAL INFORMATION

### *A. Federal Law*

There is no single, uniform federal law regulating personal data collection in the United States.[120] The Financial Services Modernization Act, included in the Gramm-Leach-Bliley Act of 1999 ("GLBA"), is the most relevant data protection law pertaining to financial institutions.[121] Specifically, Title V of the GLBA restricts financial institutions' disclosure of private consumer financial information.[122] Under Title V of the GLBA, financial institutions must (1) respect the privacy of their customers,[123] and (2) protect the security and confidentiality of their customers' nonpublic personal information.[124] These two provisions provide consumer bankers an absolute right to know how their personal

117. *See id.* ("A year down the line, however, public sentiment toward Equifax is slowly getting restored as more people begin to trust the brand again. YouGov's Buzz Metric shows that Equifax public opinion is hovering around negative two now; almost the same spot it was in before the hacking.").

118. *See Equifax to Pay $575 Million*, *supra* note 49 (discussing how the Equifax breach reached 147 million people, and that Equifax had to pay settlements amounts to all fifty states, the District of Columbia, and Puerto Rico following the breach); *see also* Wack, *supra* note 479 (saying that Capital One has to pay out $80 million after compromising the personally identifiable information of 100 million Americans and six million Canadians).

119. *See* Jolly, *supra* note 63 (discussing the "patchwork" system of laws regulating data protection in the United States).

120. Jolly, *supra* note 63.

121. Gramm-Leach-Bliley Act ("GLBA") of 1999, Pub. L. No. 106-102, 113 Stat. 1338, 15 U.S.C. § 6801 et seq. (1999); *see also* Jolly, *supra* note 63 (referring to the GLBA as one of the "most prominent federal privacy laws").

122. *Id.*; *see also* Neal R. Pandozzi, *Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, 55 U. MIAMI L. REV. 163, 164 (2001) (examining the shortfalls of Title V of the GLBA).

123. GLBA, 15 U.S.C. § 6801(a).

124. *Id.* § 6801(b).

information will be used.[125] Congress outlined a procedure in this provision of the GLBA to safeguard consumer information.[126] This procedure gives consumers the option to opt-out of information sharing with nonaffiliated third parties.[127] In addition, each financial institution is mandated to create a written privacy policy if the institution transfers consumer information to unaffiliated bank entities.[128]

Administrative agencies, such as the federal banking regulators and FTC, are tasked with ensuring compliance.[129] These agencies were left to their own discretion on what rules to promulgate to enforce Title V.[130] The Federal Deposit Insurance Corporation ("FDIC"), OCC, and the Federal Reserve Board among other agencies jointly adopted a federal privacy model.[131] The FTC, on the other hand, had the "catch-all" responsibility of enforcing the Title V provisions for "[a]ny other financial institution" not covered by the other regulators.[132] Thus, the FTC implemented two sweeping regulations: a "Financial Privacy Rule,"[133] requiring financial institutions to provide an annual notice to all consumers of the institution's privacy policies,[134] as well as a "Safeguards Rule," which forbids financial institutions from obtaining financial information through fraudulent means.[135]

Despite the additional efforts of these federal agencies and regulators, the GLBA still has pitfalls and criticisms—namely that it does

125. *See* Pandozzi, *supra* note 122, at 164–65 (examining the origins and scope of Title V of the GLBA).

126. GLBA, 15 U.S.C. § 6802.

127. *Id.* § 6802(b)(1); *see generally* William Francis Galvin, *Gramm-Leach-Bliley Act (GLBA)*, SEC'Y OF THE COMMONWEALTH OF MASS., https://www.sec.state.ma.us/sct/sctgbla/gblaidx.htm [https://perma.cc/P5QV-KNL2] (last visited Feb. 6, 2021) (defining the terms "affiliate," which is a company that controls or is under common control as the organization, and "non-affiliate," which is any entity other than the organization or an affiliate).

128. GLBA, 15 U.S.C. § 6802(b)(1); David W. Roderer, *Tentative Steps Toward Financial Privacy*, 4 N.C. BANKING INST. 209, 212 (2000).

129. GLBA, 15 U.S.C. § 6802(a).

130. *Id.* § 6804(a)(1)(A).

131. Stephen F.J. Ornstein et al., *Final Model Privacy Form Under the Gramm-Leach-Bliley Act*, 65 CONSUMER FIN. L.Q. REP. 171, 171 (2011).

132. *See* Kathleen A. Hardee, *The Gramm-Leach-Bliley Act: Five Years After Implementation, Does the Emperor Wear Clothes?*, 39 CREIGHTON L. REV. 915, 924 (2006) (examining the Federal Trade Commission's broad responsibilities in implementing the GLBA in comparison to other federal agencies).

133. 16 C.F.R. §§ 313.1–313.18 (2020).

134. *Id.* § 313.5(a)(1).

135. *Id.* § 314.

not go far enough to protect consumers.[136] For example, the GLBA offers no private right of action for affected consumers.[137] This problem is compounded by the fact that banks often collect consumer information outside the scope of protections granted by the GLBA, such as when a bank gathers information unrelated to financial services or to the opening of a checking account.[138] Additionally, the GLBA's consumer opt-out route is subject to exceptions, effectively creating an "information-sharing loophole."[139] Consequently, a current issue with the GLBA is how to protect consumer data amidst a work-from-home environment, which is a policy matter that will need to be addressed if remote work persists post-pandemic.[140]

While the GLBA is the legal backbone for data protection domestically, legislation here may have fallen behind as compared to international data protection laws.[141] There have been calls for the United States to enact a law similar to the General Data Protection Regulation ("GDPR") that took effect in the European Union ("E.U.") on May 25,

136. *See* Pandozzi, *supra* note 122, at 166 ("Several congressman and consumer groups believe that Title V does not go far enough to protect financial information. . . . [F]inancial services companies remain free to share a customer's financial information with their affiliates [despite the opportunity for consumers to opt out of information sharing with unaffiliated third parties]. Additionally, the opt-out mechanism [for consumers] is subject to certain exceptions that may create an information-sharing loophole for financial services companies.").

137. *See* Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007) (discussing the lack of relief for plaintiffs bringing forth GLBA lawsuits).

138. *See* Fara Soubouti, Note, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 534 (2020) ("[F]inancial institutions gather information about visitors to their websites or mobile applications for visits unrelated to financial services or opening of an account. Banks may then use that consumer data internally for marketing purposes and externally by selling that information to third parties.").

139. *See* Pandozzi, *supra* note 122, at 166 (discussing the shortcomings of Title V of the GLBA, namely how a financial services institution may still end up sharing personal consumer information).

140. *See* David T. Rich, *GLBA in a Work From Home Environment*, WIPFLI (Apr. 21, 2020), https://www.wipfli.com/insights/articles/fi-covid-19-glba-security-for-work-for-home-employees [https://perma.cc/7V9K-RY2M] (discussing how it is more challenging for financial institutions to reinforce the data protection provisions of the GLBA given the shift to a remote workforce in 2020).

141. *See* Katarina Rebello, *Does the U.S. Need an American Alternative to the GDPR?* TRANSATLANTIC PUZZLE (Sept. 19, 2019), https://transatlanticpuzzle.com/2019/09/19/does-the-u-s-need-an-american-alternative-to-the-gdpr/ [https://perma.cc/LJ6M-U7WP] (analyzing how American legislators are contemplating stronger data protection laws in light of the European Union's passage of the GDPR).

2018.[142] The GDPR is a data-sharing law intended to give individuals living in the E.U. rights to their personal data and how it is used and collected.[143] Failure to follow the GDPR's regulations can result in fines as high as $22.6 million or even as much as 4% of the company's annual revenue.[144]

The reach of the GDPR is not exclusive to Europe.[145] In fact, it has sweeping effects on U.S. companies.[146] According to the U.S. Secretary of Commerce, the GDPR has resulted in U.S. companies investing billions of dollars in cybersecurity in order for their privacy policies to be GDPR-compliant.[147] However, these expenditures may not be isolated occurrences.[148] Other countries are following the E.U.'s lead and are revising their own data protection laws.[149] For example, Canada amended its Personal Information Protection and Electronic Documents

142. Lauren Davis, Note, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499, 507–08 (2020).

143. *See* Richie Koch, *What Does GDPR Stand For? (And Other Simple Questions Answered)*, GDPR EU, https://gdpr.eu/what-does-it-stand-for/ [https://perma.cc/F57R-W6D7] (last visited Feb. 6, 2021) (providing background on the implementation of the GDPR); *see also* Ben Wolford, *Data Sharing and GDPR Compliance: Bounty UK Shows What Not to Do*, GDPR EU, https://gdpr.eu/data-sharing-bounty-fine/ [https://perma.cc/5V97-3S7J] (last visited Nov. 2, 2020) (discussing the requirements an organization must abide by if they want to collect consumer financial data).

144. *See* Sarah Hospelhorn, *Analyzing Company Reputation After a Data Breach*, VARONIS: INSIDE OUT SEC. BLOG (last updated Mar. 29, 2020), https://www.varonis.com/blog/company-reputation-after-a-data-breach/ [https://perma.cc/A65W-CGJW] (discussing how the GDPR's strict requirement that disclosure of a data breach must occur within seventy-two hours, or else noncompliance will result in steep fines).

145. *See* Paul M. Schwartz, *Global Data Privacy: The E.U. Way*, 94 N.Y.U. L. REV. 771, 772–73 (2019) (Proof of the influence of the GDPR and EU data protection law, however, goes beyond the hefty sums spent by U.S. companies to comply with them. The EU has taken an essential role in shaping how the world thinks about data privacy. Even corporate America draws on EU-centric language in discussing data privacy.").

146. *See id.* (stating that companies in the United States have had to invest hefty sums in order to comply with the GDPR).

147. Wilbur Ross, *EU Data Privacy Laws Are Likely to Create Barriers to Trade*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c [https://perma.cc/FW8C-YLHV].

148. *See* Todd Ehret, *Data Privacy and GDPR at One Year, a U.S. Perspective. Part Two - U.S. Challenges Ahead*, REUTERS (May 29, 2019, 11:24 AM), https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-two-u-s-challenges-ahead-idUSKCN1SZ1US [https://perma.cc/XQK5-JZUW] (examining how other countries have updated their own data privacy practices to ensure compliance with the GDPR).

149. *See id.* (examining how the rest of the world has taken notice of the European Union's adoption of the GDPR).

Act, which now significantly overlaps with the GDPR.[150] Similarly, Australia published additional guidance on its Privacy Act of 1988 to address updates triggered by the GDPR.[151] A key difference between the E.U. approach and the U.S. approach is that the latter is macro-focused.[152] Specifically, the U.S. targets its legislation towards cybersecurity and breaches, while the E.U. places its emphases on personal privacy.[153] Regardless, the GLBA merely sets a floor which permits states to enact more stringent privacy laws.[154]

### *B. State Law*

Unless a more comprehensive federal law for data privacy is enacted, data protection in the United States is dependent on a "patchwork system" of state laws.[155] While all fifty states have data breach laws, these laws require little more than just notification that a breach has occurred.[156] However, some states like New York and California have taken steps forward to improve data security and the personal privacy of its residents.[157] New York's Department of Financial Services ("NYDFS") has enacted a set of cybersecurity regulations targeted specifically at financial institutions known as "Reg 500."[158] These regulations were created to guard against the threat posed by cybercriminals and to protect consumers from intrusion upon their private

150. *Id.*

151. *Id.*

152. *See id.* ("Public and political emphasis on privacy so far in the United States has been focused on breaches and cybersecurity, as opposed to the European approach which has centered on personal privacy.").

153. *Id.*

154. *See* Soubouti, *supra* note 138, at 530 (discussing the interplay between federal and state privacy laws).

155. Jolly, *supra* note 63.

156. *Id.*

157. *See* Davis, *supra* note 142 (discussing the adoption and implementation of the California Consumer Privacy Act); *see also How to Meet DF 23 NYCRR 500 Cyber Security Regulation*, MAUREEN DATA SYS., https://www.mdsny.com/how-to-meet-dfs-23nycrr-500-in-five-steps/ [https://perma.cc/L93M-JHUR] (last visited Nov. 3, 2020, 9:17 PM) (discussing a set of cybersecurity regulations applicable to financial institutions in New York).

158. 23 N.Y. COMP. CODES R. & REGS. tit. § 500 *et seq*. (2017); Damon W. Silver & Catherine R. Tucciarello, *NYDFS Files First Enforcement Action Under Reg 500*, NAT. L. REV. (Aug. 17, 2020), https://www.natlawreview.com/article/nydfs-files-first-enforcement-action-under-reg-500 [https://perma.cc/G5E8-QM7M].

financial data.[159] Reg 500 sets a regulatory minimum standard for cybersecurity that allows companies to build upon in assessing their own specific risk profiles.[160] This law requires financial service companies to maintain a cybersecurity policy addressing, but not limited to, the following areas: data governance, customer data privacy, systems and network security, risk assessment, and incident responses.[161] Reg 500 took effect in 2007 and the NYDFS just filed its first enforcement action in July 2020.[162] Meanwhile, only California has enacted a broader data protection and privacy law.[163]

California has passed the most comprehensive state data protection law: the California Consumer Privacy Act ("CCPA").[164] In fact, the CCPA has been dubbed with the nickname "GDPR-lite" and the "California GDPR."[165] The CCPA provides consumers with four key rights: (1) the right to know, (2) the right to be forgotten, (3) the right to opt out, and (4) the right to equal service and price.[166] Any business that collects personal information of California residents is subject to its provisions, including financial institutions.[167] While it is still too early to gauge the CCPA's long-term impact, companies both in the United States and across the world are asking for more time to comply in putting their new privacy practices in place.[168] Despite pleas from both U.S.-based

159. *How to Meet DF 23 NYCRR 500 Cyber Security Regulation*, MAUREEN DATA SYS., https://www.mdsny.com/how-to-meet-dfs-23nycrr-500-in-five-steps/ [https://perma.cc/L93M-JHUR] (last visited Nov. 3, 2020, 9:17 PM).

160. N.Y.C. BAR ASS'N, NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES 23 NYCRR 500 CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES, 20190613a NYCBAR 131 (2019).

161. 23 N.Y. COMP. CODES R. & REGS. tit. § 500.03.

162. *See* Silver & Tucciarello, *supra* note 153 (scrutinizing the New York Department of Financial Services's first enforcement action against First American Title Action Company, who inadvertently exposed personally identifiable information of its consumers by failing to mitigate a security vulnerability on its website).

163. *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2020); Jolly, *supra* note 63 ("In July 2018, California passed the most comprehensive data protection law in the US[.]").

164. *See generally* Davis, *supra* note 142 (discussing the adoption and implementation of the California Consumer Privacy Act).

165. Ehret, *supra* note 137.

166. Davis, *supra* note 142, at 506.

167. CAL. CIV. CODE § 1798.100.

168. *See* Robert B. Milligan et al., *The Impact of COVID-19 on the California Consumer Privacy Act*, SEYFARTH (Apr. 7, 2020), https://www.seyfarth.com/print/content/43301/the-impact-of-covid-19-on-the-california-consumer-privacy-act-2.pdf [https://perma.cc/9M4U-52QZ] (examining the impact COVID-19 will have on the enforcement of the California

and international companies for more time to absorb the shock of compliance, the California Attorney General is resolute—no one gets extra time.[169] However, the CCPA's collection and storage policies may have been complicated by novel situations arising out of the pandemic.[170] Businesses are now collecting physiological data of consumers, such as body temperature, prior testing results, and contact tracing via cell phones.[171] The nature of how to collect, store, and maintain that personal data is unaddressed in the CCPA, proving that privacy laws need to be continuously updated to reflect the changing times.[172]

Since California took a strong stance to ensure personal privacy protection, sixteen other states have introduced comprehensive state privacy bills—a sign that the "patchwork system" may be improved.[173] Moreover, Congress has proposed the COVID-19 Consumer Data Protection Act, which would (1) provide Americans more transparency over their personal data like health records and location data, and (2) hold businesses accountable if they use such personal data to fight the pandemic.[174] This bill takes GDPR-esque steps by zeroing in on personal privacy protections.[175] One of the sponsors of the bill, Senator Jerry

---

Consumer Privacy Act, with the pandemic having created novel data protection situations that companies will have to confront).

169. *See id.* (discussing the uncertainty surrounding how companies will enforce the CCPA, which is made even more troublesome with the regulations pertaining to the CCPA having not been finalized yet).

170. *See id.* (stating that novel situations include the increased need for companies to collect physiological information of consumers, such as body temperature, prior COVID-19 testing results, and contact tracing).

171. *Id.*

172. *See id.* ("At least some light should be shed on these [referring to the collection of physiological data during the pandemic] and other CCPA-related questions once the regulations finalized and provided to the public, though the litigation ensuing from the CCPA will only increase with time, and with pandemic-related new realities.").

173. *See* Soubouti, *supra* note 138, at 531 ("The California Consumer Privacy Act ("CCPA") is currently the most protective comprehensive state data privacy law in the country. As of October 2019, sixteen other states have introduced comprehensive state privacy bills to enhance consumer data protections of their residents.").

174. *See* Press Release, Wicker, Thune, Moran, Blackburn Announce Plans to Introduce Data Privacy Bill, U.S. S. Comm. on Commerce, Sci., & Transp. (Apr. 30, 2020) (examining how the proposed bill is meant to specifically address data protection issues arising as a result of the COVID-19 pandemic).

175. *See id.* ("It is paramount that as tech companies utilize data to track the spread of COVID-19, Americans' privacy and security are not put at risk. Health and location data can reveal sensitive and personal information, and these companies must be transparent with their users.") (examining the proposed data privacy bill, the COVID-19 Consumer Data Protection

Moran, states that Congress still needs to enact a uniform data privacy law.[176]

## IV. THE PRESENT IMPACT OF COVID-19 ON THE BANKING INDUSTRY

### *A. How the Pandemic Changed the Landscape of Banking*

"Before COVID-19, these types of digital applications were nice to have. Now it's a *necessity*."[177] This statement made by Anne Chow, the chief executive officer of AT&T, reflects how digital applications have become a lifeline for every bank during the pandemic as social distancing protocols have interrupted regular operations.[178] The Department of Homeland Security deemed the financial services sector a Critical Infrastructure Sector during the COVID-19 pandemic, which means financial services workers have a "special responsibility" to maintain their normal work schedules.[179] However, banks have had to adopt new ways to continue their operations while ensuring their adherence to public health and safety guidelines.[180]

Adapting to a "new normal" has forced banks to restrict in-person consumer access.[181] For instance, the FDIC has allowed its member

---

Act, which is aimed at ensuring consumers have control over their physiological and geographic data).

176. *Id.*

177. Anne Chow, *COVID-19: An Economic Crisis as well as a Pandemic – Technology is Here to Help*, AT&T: TECH. BLOG (Apr. 28, 2020), https://about.att.com/innovationblog/2020/04/covid_19_technology.html [https://perma.cc/42GH-FH3E] (emphasis added) (detailing how AT&T has assisted financial services organizations transition to a remote workforce and to a social distanced work environment during the pandemic).

178. *See id.* ("Everything that could move online, did move online. The economy, businesses and consumers depended on and needed this transformation to survive.").

179. *See* Memorandum from Secretary Steven T. Mnuchin, Dep't of the Treasury, Memorandum for Financial Services Sector (Mar. 22, 2020), https://www.aba.com/-/media/documents/incident-response/Financial-Services-Sector-Essential-Critical-Infrastructure-Workers.pdf [https://perma.cc/MJN4-RZC2] (explaining which workers are part of the Essential Critical Infrastructure Workforce in the financial services sector).

180. OFF. OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. NO. 2020-23, PANDEMIC PLANNING: ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS IN THE FINANCIAL SERVICES SECTOR (Mar. 25, 2020), https://www.occ.treas.gov/news-issuances/bulletins/2020/bulletin-2020-23.html [https://perma.cc/V56J-H7UK] (clarifying which employees in the workforce are considered essential and providing advice on how companies can continue business operations during the pandemic).

181. *See* FED. DEPOSIT INS. CORP., FREQUENTLY ASKED QUESTIONS FOR FINANCIAL INSTITUTIONS AFFECTED BY THE CORONAVIRUS DISEASE 2019 (REFERRED TO AS COVID-19)

banks to limit consumer access to physical branch offices.[182] Similarly, the OCC has recognized that, considering the pandemic, there may be temporary bank closures and limited access to in-person services.[183] Needless to say, the financial services industry has had to increasingly rely on technology to continue operating their businesses remotely.[184]

The pandemic has also spawned unprecedented levels of telework.[185] For example, 84% of Deutsche Bank's investment banking division is currently working remotely.[186] JPMorgan Chase is alternating its 60,950 employees between office and remote work for an indefinite period of time.[187] As telework surges, the OCC recommends that remote bank employees be extra vigilant and use secure communications while working at home.[188] The recommended measures include using virtual

(May 27, 2020), https://www.fdic.gov/coronavirus/faq-fi.pdf [https://perma.cc/WK34-22HH] (stating that financial institutions can consider alternative methods to physical banking in order to continue providing services to customers).

182. *See id.* at 4 ("Financial institutions can consider alternative service options to provide access to financial services. Financial institutions may want to remind customers of the various ways they can access banking services without physically coming to a facility, such as managing their accounts online, performing transactions at an automated teller machine (ATM), using telephone banking, or accessing a mobile banking application.").

183. *See Coronavirus Disease 2019 (COVID-19) Frequently Asked Questions for National Banks and Federal Savings Associations*, OFF. OF THE COMPTROLLER OF CURRENCY, https://www.occ.gov/topics/supervision-and-examination/bank-operations/covid-19-information/covid-19-faqs-for-national-banks-and-fsa.html#BankOperations [https://perma.cc/T9GD-ZKWB] (last updated June 15, 2020) [hereinafter *Coronavirus Disease 2019*].

184. *See* Mo Katibeh & Steve Canepa, *AT&T and IBM: Helping Businesses Adapt to New Work Environments*, AT&T: TECH. BLOG (Aug. 18, 2020), https://about.att.com/innovationblog/2020/08/att_ibm.html [https://perma.cc/6Q2Z-7ZDL] (detailing how digital technologies will be critical for various industries in the post-pandemic future).

185. *See* Katherine Guyot & Isabel V. Sawhill, *Telecommuting Will Likely Continue Long after the Pandemic*, BROOKINGS INST. (Apr. 6, 2020), https://www.brookings.edu/blog/up-front/2020/04/06/telecommuting-will-likely-continue-long-after-the-pandemic/ [https://perma.cc/4JTD-2PY3] (discussing how telework has skyrocketed because of the pandemic, a trend that will likely become permanent post-pandemic).

186. *See Retail Banking in the Age of COVID*-19, DELOITTE 12 (May 2020), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-retail-banking-in-the-age-of-covid-19.pdf [https://perma.cc/3SYD-RK2G] (analyzing how COVID-19 will affect the banking industry).

187. *See* Hugh Son, *JPMorgan Will Have Staff Cycle Between Office and Remote Work in a Move That May Remake Wall Street*, CNBC, https://www.cnbc.com/2020/08/25/jpmorgan-will-have-staff-cycle-between-office-and-remote-work-in-a-move-that-may-remake-wall-street.html [https://perma.cc/F92D-E565] (last updated Aug. 25, 2020, 1:45 PM) (discussing JPMorgan's plan to alternate its workforce between in-person and remote work).

188. *See Coronavirus Disease 2019, supra* note 183 ("Banks should remind employees that *cyber criminals are very active during these times of stress*. Remind employees of good

private networks ("VPNs"), appropriately storing sensitive information, not opening emails from unknown sources, and conducting phone conversations with customers in a safe environment.[189]

While the pandemic has presented an opportunity for increased telework, it has also presented a crisis through the increased number of cyberthreats.[190] Therefore, cybersecurity is more important than ever.[191] In addition, history shows that there is a correlation between increased cybercrime and economic turmoil.[192] Indeed, cybercrime reportedly increased 33% during the 2008 financial crisis.[193] Just in the first quarter of 2020, the number of data breaches is up 273% compared to last year.[194] Undoubtedly, hackers are capitalizing on the upheaval and fear caused by the virus.[195]

### A. *What Data Breaches Have Occurred During the COVID-19 Pandemic?*

Cybercriminals have wasted no time in capitalizing on the government's efforts to blunt the economic distress.[196] In an effort to

---

cybersecurity practices such as not opening email or documents from unknown sources or clicking on unknown links. Be extra vigilant by using call-backs or verbal confirmation with bank staff and customers") (emphasis added).

189. *See id.* ("Employees working from home should use secure communications, such as a virtual private network (VPN), when working with sensitive information. Employees should appropriately store and safeguard sensitive information while working at home. Telephone conversations dealing with sensitive customer or employee information should be guarded in a home environment. Bank management should provide consistent and clear guidance on how to handle sensitive customer, bank, and employee information to all employees working at homes.").

190. *See Remote Work in 2021: Cybersecurity Grows in Importance*, DICE (Nov. 13, 2020), https://insights.dice.com/2020/11/13/remote-work-in-2021-cybersecurity-grows-in-importance/ [https://perma.cc/ZY5R-NX8P] (discussing how significant populations of employees will remain working remotely in 2021, and COVID-19 has brought about a plethora of cybersecurity issues in the work-from-home-environment).

191. *See* RISK BASED SEC., INC., *supra* note 21 (examining how the conditions are perfect in a pandemic for increased cybercrime).

192. *See id.* (reporting that Internet fraud increased during the 2008 recession).

193. *See id.* (examining various news sources reporting on the surge of cybercrime during the 2008 recession).

194. *See* Sheng, *supra* note 1 (discussing how cybercriminals capitalize on uncertainty and confusion during times of upheaval, with the number of breaches up 273% in the first quarter of 2020 compared to 2019 as companies shifted to online business).

195. *See id.* (scrutinizing the ways in which cybercriminals have taken advantage of the COVID-19 pandemic by hacking the government and businesses).

196. *See* Nathaniel Popper, *'Pure Hell for Victims' as Stimulus Programs Draw a Flood of Scammers*, N.Y. TIMES, https://www.nytimes.com/2020/04/22/technology/stimulus-

mitigate the economic fallout resulting from COVID-19, the government has issued trillions of dollars in relief funds through their COVID-19 response bill legislation (the "CARES Act").[197] The most visible relief has been in the form of Economic Impact Payments ("EIP"), also known as stimulus checks.[198] Eligible taxpayers—individuals whose income was below $99,000—received a one-time EIP payment of $1,200.[199] Joint households whose income was below $198,000 received a one-time EIP payment of $2,400.[200] Unfortunately, the availability of stimulus funds "ring[s] the dinner bell for hackers."[201] Cybercriminals have assumed false identities and set up malicious websites to steal these stimulus funds.[202] Indeed, despite the global health crisis, cybercrime is speeding up.[203] Total traffic at the Identity Theft Resource Center, a nonprofit organization that helps data breach victims, was up 850% in March compared to 2019.[204] The FTC reported increased cases of identity fraud since the pandemic started.[205] Federal agencies like the Federal Bureau of Investigation have even issued warnings of cybercriminals attempting to capitalize on the pandemic.[206]

---

checks-hackers-coronavirus.html [https://perma.cc/ZFL4-8B7Q] (last updated Sept. 15, 2020) (examining how cybercriminals have been targeting recipients of stimulus payments to help blunt the economic fallout of COVID-19).

197. *Id.*; *see also* Coronavirus Aid, Relief, and Economic Security Act ("CARES Act"), Pub. L. No. 116-136, 134 Stat. 281 (2020).

198. *See* Popper, *supra* note 196 (discussing how cybercriminals are targeting stimulus check recipients); *see also* 26 U.S.C. § 6428 (providing COVID-19 relief through payments of $1,200 for eligible individuals or $2,400 for eligible individuals filing a joint return, in addition to $500 per child under the age of 17).

199. *See* 26 U.S.C. § 6428; U.S. Dep't of the Treas., *The CARES Act Provides Assistance to Workers and Their Families*, POLICY ISSUES: CARES ACT-ASSISTANCE FOR WORKERS AND FAMILIES https://home.treasury.gov/policy-issues/cares/assistance-for-american-workers-and-families [https://perma.cc/S6SH-GX4S] (providing details on who is eligible for Economic Impact Payments and the amount eligible taxpayers can expect to receive); *see also* Jessica Dickler & Lorie Konish, *Will Americans Get Another Round of Stimulus Payments? Your Top Questions Answered.* CNBC, https://www.cnbc.com/2020/06/22/will-americans-get-more-stimulus-payments-your-top-questions-answered.html [https://perma.cc/F9SA-2YXG] (last updated June 22, 2020, 4:49 PM) (discussing the number of Americans who have received stimulus payments, and who is eligible for a stimulus payment).

200. *Id.*

201. Popper, *supra* note 196.

202. *See id.* (reporting an uptick in cybercrime during the pandemic).

203. *Id.*

204. *Id.*

205. *Id.*

206. FED. BUREAU OF INVESTIGATION, PUB. SERV. ANNOUNCEMENT I-042020-PSA, ONLINE EXTORTION SCAMS INCREASING DURING THE COVID-19 CRISIS (Apr. 20, 2020); *see also* Ken

While individuals and families have suffered from cybercrime during the pandemic, federal agencies have also been hurt.[207] On March 25, 2020, the Small Business Administration discovered a data breach that compromised the information of 7,913 businesses applying for the Economic Injury Disaster Loan ("EIDL") program.[208] The EDIL program offers each applicant up to $2 million in loans.[209] It was the only source of emergency funding for many businesses before Congress enacted the $2 trillion CARES Act to provide COVID relief.[210]

Bank of America suffered from a data breach on April 22, 2020, impacting customers who applied for the Paycheck Protection Program;[211] another program created by the CARES Act to encourage businesses to keep employees on its payroll.[212] Saying that only a "small number" of customers were affected, Bank of America has not disclosed the specific number of breached applications.[213] In response to the breach, Bank of America (1) ordered an investigation, (2) advised clients to review their account statements carefully and report suspicious activity, and (3) offered clients free two-year membership of Experian's identity theft program.[214]

---

Dilanian et al., *FBI, Other Agencies Warn of 'Imminent Cybercrime Threat' to U.S. Hospitals*, NBC NEWS, (Oct. 28, 2020, 11:32 PM), https://www.nbcnews.com/news/us-news/fbi-other-agencies-warn-imminent-cybercrime-threat-u-s-hospitals-n1245212 [https://perma.cc/ZXS5-WUV5] (discussing how federal agencies like the Federal Bureau of Investigations are warning of "an increased and imminent cybercrime threat").

207. Patrick McKnight, *SBA Loan Program Suffers Data Breach*, AMERICAN BAR ASS'N (May 6, 2020), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2020/202005/fa_1/ [https://perma.cc/R4TN-U3WC] (detailing a data breach suffered by Economic Injury Disaster Loan program through the United States Small Business Administration, which involved 7,913 businesses applying for emergency funding as a result of COVID-19).

208. *Id.*

209. *Id.*

210. Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") Pub. L. No. 116-136, 134 Stat. 281 (2020); McKnight, *supra* note 207.

211. Dev Kundaliya, *Bank of America Suffers Data Breach in Paycheck Protection Program,* COMPUTING (May 28, 2020), https://www.computing.co.uk/news/4015730/bank-america-suffers-breach-paycheck-protection-program-application-process [https://perma.cc/4MJY-3X8D].

212. *See Paycheck Protection Program*, SMALL BUS. ADMIN., https://www.sba.gov/funding-programs/loans/coronavirus-relief-options/paycheck-protection-program [https://perma.cc/KQ3U-NQ42] (last visited Nov. 2, 2020) (discussing details and eligibility criteria of the Paycheck Protection Program).

213. Kundaliya, *supra* note 211.

214. *Id.*

## V. THE FUTURE IMPACT OF COVID-19 ON THE BANKING INDUSTRY

The increased rate of cybercrime coincides with a time in which there is a greater push for employees to work remotely.[215] In fact, a group of U.S. senators stated: "Telework protects not only federal employees from the spread of COVID-19, but also their families and the communities across the country in which they work."[216] This sentiment proposes a federal stamp of approval on a growing practice: the maximization of telework.[217] This was arguably the first time that telework is lauded not just because it is convenient but also because it is a good public health safety measure.[218] The shift to remote work—for both public and private sectors—has been well received.[219] Survey data reports that 98% of workers would like to work-from-home permanently.[220] Companies including Twitter, Slack, and Square have already announced a work-from-home forever option for their employees.[221] Facebook expects half of its 48,000 employees to work-from-home throughout the next ten years.[222] Additionally, several

215. *See* Letter from Chris Van Hollen to Senate Majority Leader Mitch McConnell and Minority Leader Charles Schumer, (July 31, 2020). https://www.vanhollen.senate.gov/imo/media/doc/Letter%20to%20Leadership%20on%20Telework%20Provision%20in%20C4%20Final%20version.pdf [https://perma.cc/7XQR-M6LQ] (discussing the need to keep employees at home during the pandemic).

216. *Id.*

217. *See id.* (urging the Senate to maximize telework in order to stop the spread of COVID-19).

218. *See id.* (discussing how, in light of an increasing number of COVID-19 cases, federal agency employees must set a positive example for other workers by taking precautionary measures like working remotely).

219. *See* Nick Routley, *6 Charts that Show That Employers and Employees Really Think About Remote Working*, WORLD ECON. F. (June 3, 2020), https://www.weforum.org/agenda/2020/06/coronavirus-covid19-remote-working-office-employees-employers [https://perma.cc/GMU8-TWRZ] (examining attitudes towards remote work during the pandemic, and how 98% of those surveyed would prefer to still be able to work-from-home post-pandemic).

220. *See id.* (reporting that the 98% of those surveyed said the top benefits of working-from-home include, but are note limited to, more flexible schedules, the ability to work from any location, being able to spend more time with family, and the lack of a commute).

221. *See* Dana Brownlee, *Twitter, Square Announce Work From Home Forever Option: What Are The Risks?* FORBES (May 18, 2020, 8:08 PM), https://www.forbes.com/sites/danabrownlee/2020/05/18/twitter-square-announce-work-from-home-forever-optionwhat-are-the-risks/#62c9f2092565 [https://perma.cc/XJ34-CZ7A] (discussing how companies are changing their telework policies in light of the sure in telework during the pandemic).

222. *See* Shannon Bond, *Facebook Expects Half Its Employees to Work Remotely Permanently*, NPR (May 21, 2020, 5:15 PM), https://www.npr.org/sections/coronavirus-live-

companies like Shopify and Box anticipate having permanent work-from-home options in the future.[223] Remote work is projected to stay in the post-pandemic world.[224]

However, the reality of the transition to remote work during the pandemic is less than ideal.[225] Scores of financial institutions were ill equipped to make the transition to remote work.[226] Many information technology ("IT") departments were not prepared to handle the substantial increase in remote employees and third-party vendors.[227] Employees were not prepared for the transition either.[228] A survey of remote workers shows that 72% are not working from a dedicated home office space.[229] Instead, their living rooms and bedrooms serve as their "office."[230] Moreover, 40% of remote workers are not even working from an actual desk.[231]

---

updates/2020/05/21/860382831/facebook-expects-half-its-employees-to-work-remotely-forever [https://perma.cc/KP5F-LL42] (detailing new work-from-home policies that companies are developing in light of COVID-19).

223. *See* Rob McLean, *These Companies Plan to Make Working From Home the New Normal. As in Forever*, CNN BUS., https://www.cnn.com/2020/05/22/tech/work-from-home-companies/index.html [https://perma.cc/F4J4-2QHV] (last updated June 25, 2020) (discussing how different companies are changing work-from-home policies, and the possibility that working from home may become a permanent fixture post-pandemic).

224. *See Remote Work in 2021: Cybersecurity Grows in Importance*, *supra* note 185 ("[S]urvey results show that even as organizations are preparing for a return to physical offices in 2021, remote and home-office work is likely here to stay for the long-term for a good portion of the employees.").

225. *See* Evan Sparks, *The Telework-Ready Bank*, A.B.A. BANKING J. (Apr. 3, 2020), https://bankingjournal.aba.com/2020/04/the-telework-ready-bank/ [https://perma.cc/LNT6-YPCE] (discussing considerations banks should take into account as they transition to remote work).

226. *See* Ann Marie Uetz et al., *Managing the Commercial Impact of the Coronavirus: Implications for Remote Working and Data Security*, NAT'L L. REV. (Mar. 12, 2020), https://www.natlawreview.com/article/managing-commercial-impact-coronavirus-implications-remote-working-and-data-security [https://perma.cc/BF3Y-WWQV] (providing guidance on how companies can manage a remote workforce).

227. *See id.* (stating that the unique circumstances of the pandemic are not conditions that most IT departments are prepared to deal with).

228. *See* Chris Westfall, *Statistics Show Remote Workers Are Frustrated, Many Still Unprepared for Working From Home*, FORBES (Aug. 25, 2020, 3:40 PM), https://www.forbes.com/sites/chriswestfall/2020/08/25/statistics-show-remote-workers-are-frustrated-many-still-unprepared-for-working-from-home/#323fb2f548b3 [https://perma.cc/LY3B-Q8WR] (using statistical data from the company Nulab to show how many employees were not prepared for the shift to remote work).

229. *Id.*

230. *Id.*

231. *Id.*

People change their behaviors when they transition from an office environment to a home environment.[232] Therefore, the key concern with a surge in telework is maintaining a safe cybersecurity environment.[233] The risk of data harms stems not only from cybercriminals but also from employees themselves.[234] A study conducted by the security firm Tessian found that 48% of employees are less likely to follow safe data practices at home.[235] An alarming 52% of those surveyed said they believed they could get away with riskier behavior,[236] such as using public hotspots and unsecure networks.[237]

These risks associated with unsupervised telework include, but are not limited to, unsecure networks, phishing attacks, computer sharing, and insecure devices.[238] Employees may have weaker protocols in their homes, like using WEP (the weakest protocol and highly vulnerable to attacks) instead of WPA-2 (the most secure protocol) in securing their Wi-Fi networks.[239] If a remote workforce is to be a permanent

232. *See* Sparks, *supra* note 225 (discussing how the shift in behavior when transitioning to a work-from-home environment "creates an opportunity for threat actors" to hack into computer systems).

233. *See id.* (discussing how banks should have cybersecurity measures in place and should consider novel cybersecurity issues while employees work from home).

234. *See* Aman Kidwai, *Employees Working From Home May Present a Threat to Cybersecurity*, HR DIVE (May 28, 2020), https://www.hrdive.com/news/employees-working-from-home-may-present-a-threat-to-cybersecurity/578761/ [https://perma.cc/4HMV-RWCS] (examining how employees change behaviors when working remotely, such as becoming lax on proper cybersecurity practices).

235. *Half of Employees Abandon Safe Data Practices When Working Remotely, According to New Data*, REALWIRE (May 28, 2020), https://www.realwire.com/releases/Half-of-Employees-Abandon-Safe-Data-Practices-When-Working-Remotely [https://perma.cc/3VUT-UCY9] [hereinafter *Half of Employees Abandon Safe Data Practices*].

236. *Id.*

237. *See* Jason Glassberg, *Are Remote Workers a Security Risk to Your Business?* THE BUS. J. (Mar. 19, 2020, 3:05 AM), https://www.bizjournals.com/bizjournals/how-to/technology/2020/03/are-remote-workers-a-security-risk-to-your.html [https://perma.cc/67Z6-22MD] (examining cyber risks involved with telecommuting like insecure Wi-Fi networks, vulnerable software, public hotspots, and the surge in email scams).

238. Nicky Daly*, 7 Tips for Avoiding Remote Work Security Risks*, WRIKE: REMOTE WORKING (Apr. 6, 2020), https://www.wrike.com/blog/tips-avoid-remote-work-security-risks/ [https://perma.cc/F3YG-A9PC] (discussing the cybersecurity risks associated with remote work).

239. *See* Carrie Rubinstein, *Beware: Remote Work Involves These 3 Cybersecurity Risks*, FORBES (Apr. 10, 2020, 2:07 PM), https://www.forbes.com/sites/carrierubinstein/2020/04/10/beware-remote-work-involves-these-3-cyber-security-risks/#29752e6d61c4 [https://perma.cc/X3PM-HQ65] (listing three hazards of remote work: home Wi-Fi security, phishing scams, and insecure passwords).

consequence of the COVID pandemic, then cybersecurity protocols for bank employees must be revised and improved.

## VI. RECOMMENDATIONS FOR NAVIGATING BANKING POST COVID-19

COVID-19 has accelerated technology usage and increased the popularity of contactless payments.[240] The CEO of Israel's oldest bank, Bank Leumi, has stated that the days of consumers visiting bank branches and consulting bankers in-person is "passé."[241] Therefore, financial institutions will need to be digital-ready.[242] Banks need to make large investments in digital technology to improve their cyber-resiliency as the industry shifts away from a physical banking structure.[243]

Digital transformation is an ongoing process whereby businesses adapt to changes in customers and markets by leveraging digital competencies.[244] Being "digital-ready" could include: (1) banks integrating technologies like artificial intelligence or robotics into daily operations;[245] (2) banks promoting and improving use of banking functions (e.g. withdrawing money or applying for loans) through online

240. *See* Jan Bellens, *Four Ways COVID-19 is Reshaping Consumer Banking Behavior*, EY (Aug. 31, 2020), https://www.ey.com/en_us/banking-capital-markets/four-ways-covid-19-is-reshaping-consumer-banking-behavior [https://perma.cc/28NH-Q2XD] "With many companies closing their brick and mortar channels, consumers are going online to buy essentials. At the same time, concerns have been raised about whether physical cash could spread the coronavirus. This has contributed to a 57% fall in cash usage among respondents, alongside a rise in payments using credit cards (7% net), debit cards (10% net) and online payment tools (14% net).").

241. Francesca Cassidy, *What is the Future of Banking?* RACONTEUR (May 1, 2019), https://www.raconteur.net/finance/future-banking [https://perma.cc/C8PX-JC8G].

242. *See id.* (discussing how digitalization is essential for a bank's survival).

243. *See* Oliwia Berdak, *Predictions 2021: Banks Will Need To Get To Know Their Customers (Again)*, FORRESTER (Oct. 21, 2020), https://go.forrester.com/blogs/banking-predictions-2021/ [https://perma.cc/7EU5-YKQH] (predicting that the digital banking behaviors of consumers will persist post-pandemic, and that bank executives will face pressure to pivot towards digital banking).

244. ANDREW BUSS ET AL., THE DIGITAL READY BANK: HOW READY ARE EUROPEAN BANKS FOR A DIGITAL WORLD 6 (Int'l Data Corp., ed., 2016), https://st.ilsole24ore.com/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2016/07/22/IDC-WP.pdf [https://perma.cc/HXT7-WWKV].

245. *See* Chris Skinner, *Survey: Banks Just Aren't Ready for Digital*, FINANSER (Jan. 23, 2020), https://thefinanser.com/2020/01/survey-banks-just-arent-ready-for-digital.html/ [https://perma.cc/4PF7-9FKR] (stating most banks have not yet incorporate robotics into their operations); *see also* Penny Crossman et al., *10 Ways Technology Will Change Banking in 2019*, AM. BANKER (Jan. 6, 2019, 10:00 PM), https://www.americanbanker.com/list/10-ways-technology-will-change-banking-in-2019 [https://perma.cc/QFM4-HYR7] (reporting that U.S. Bank and Wells Fargo are already incorporating automations into their operations).

platforms like smartphones;[246] (3) banks opting to go paperless;[247] and finally (4) banks recognizing a minimal need for direct interaction with clients given the array of digital platforms for communication.[248] Now more than ever, it is important to have financial service organizations invest in the best technology available especially for remote-work capabilities such as 5G networks, VPNs, document capture, digital signatures, and mobile channels for banking.[249] Implementing and continually improving banking technologies will cater to the growing number of "digital-first, branch-second approach" consumers.[250]

First, banks need to perfect their mobile banking. Indeed, the pandemic is hastening the pace at which banks are converting to online platforms.[251] For example, Bank Leumi expanded to create Pepper, Israel's first mobile-only bank.[252] Built off of the customer base of Bank Leumi, Pepper has been able to circumvent consumer trust issues by building its reputation off the success of its parent company.[253] Pepper might actually be more popular than its parent company[254] because it has opened more accounts per day than Bank Leumi.[255] Moreover, Barclays launched a fully online bank in the United States, and regional banks like

246. *See* Cassidy, *supra* note 241 ("Digital tools have become people's first choice [for banking].").

247. *See Going Digital: The Banking Transformation Roadmap*, KEARNEY, https://www.es.kearney.com/financial-services/article?/a/going-digital-the-banking-transformation-roadmap [https://perma.cc/YUJ5-CLLC] [hereinafter *Going Digital*] (last visited Sept. 13, 2020) (discussing recommendations for a bank's digital vision, which includes going fully paperless).

248. *See id.* (stating that there is a "minimal need for call centers and direct interaction with clients" when mobile banking).

249. *See* Bellens, *supra* note 240 (reporting that 43% of surveyed consumers say the way they bank has changed due to the pandemic, leading to an increase in digital banking).

250. *See* Acton, *supra* note 82 (discussing how millennials are more likely to consider digital forms of banking, especially in light of their distrust of financial institutions); *see also Going Digital*, *supra* note 247 ("to keep up in this fast-changing market, traditional banks will have to adapt their operating models. In particular, changes in IT, new products and services development, and changing expectations for time-to-market will be key factors going forward.").

251. *See* Cassidy, *supra* note 241 (stating that digitalization is necessary for banks to survive in the modern age).

252. *Id.*

253. *Id.*

254. *See* Laura Noonan, *Bank Leumi to Launch Online Bank Pepper in US*, FIN. TIMES (Nov. 19, 2018), https://www.ft.com/content/810368b2-e98c-11e8-885c-e64da4c0f981 [https://perma.cc/AMW9-VV42] (discussing the Israeli-listed Bank Leumi's launch of its online-only bank Pepper).

255. *Id.*

Capital One anticipate launching online spin-off institutions.[256] Given the majority of consumers that prefer a digital relationship with their bank, [257] there is an advantage for banks in deferring to online banking platforms.[258] With less overhead needed for operating a digital platform, banks could entice new customers by offering lower fees and higher interest rates on checking accounts.[259]

Second, banks need to develop a work-from-home operating model. Some companies are already ahead of the game.[260] For instance, JPMorgan Chase has developed a pilot program dubbed "Project Kennedy," which calls for 10% of its 127,135 employees to work from home.[261] Project Kennedy is meant to serve as a contingency plan in the event that COVID-19 leads to more disruptions to in-person banking.[262] The plan will be in effect for an indeterminate period of time.[263] Pilot work-from-home programs like Project Kennedy can provide banks with the confidence and experience when dealing with a remote workforce.[264] JPMorgan Chase has already seen a significant increase in revenue and net income since implementing its work-from-model.[265] Their success can provide an incentive for other banks to work towards the same.

---

256. *Id.*

257. Yu & Hughes, *supra* note 83.

258. *See id.* ("[T]o meet customers' digital wants and needs -- and to save money -- many banks are aggressively expanding digital channels.").

259. *See* Knueven, *supra* note 84 ("There are a few reasons why online-only banks like Betterment, Wealthfront and Ally have captured tech-savvy consumers: lower fees, higher interest rates, and perhaps most importantly, convenience.").

260. *See* Michelle F. Davis, *JPMorgan Tests U.S. Virus Plan with Thousands Working From Home*, BLOOMBERG (Mar. 3, 2020, 2:41 PM), https://www.bloomberg.com/news/articles/2020-03-03/jpmorgan-tests-u-s-virus-plan-with-thousands-working-from-home [https://perma.cc/4S49-N6DF] (discussing JP Morgan Chase's pilot remote work project).

261. Jack Kelly, *JPMorgan Asked Thousands of Employees To Work From Home: This May Start a New Trend*, FORBES (Mar. 4, 2020, 2:18 PM), https://www.forbes.com/sites/jackkelly/2020/03/04/jpmorgan-asked-thousands-of-employees-to-work-from-home-this-may-start-a-new-trend/#46dfd64d48ae [https://perma.cc/8A4L-CPU7]; Davis, *supra* note 260.

262. Davis, *supra* note 260.

263. *See id.* (reporting no definite end date for Project Kennedy).

264. *See id.* ("For the consumer bank, testing the telecommuting policy on a sampling of employees across businesses can ensure kinks are worked out before the plan needs to be rolled out more broadly in the event of a pandemic…").

265. *See* Ennis, *supra* note 47 (reporting that JP Morgan Chase posted a 32% increase in revenue and 86% increase in net income).

A potential operating model could incorporate a hybrid of remote and in-person work.[266] Specifically, banks could alternate portions of its employees between at-home and in-person roles, while also offering a permanent work-from-home option for certain employees.[267] This hybrid model would reduce the need for a large office space since a smaller portion of the bank's workforce would be on-site at any given time.[268] The need for designated workstations for employees would also decrease.[269] It would be more practical to provide employees with temporary workstations as opposed to designated permanent spaces.[270] Maintaining a hybrid telework model would guarantee that banks are up-to-date with the newest technologies and have well equipped information technology departments.[271] Given that increased digitalization also increases the risk of cyberattacks, telework incentivizes banks to maintain up-to-date systems and remain vigilant against cyber-risks.[272] The key elements in implementing this hybrid model could include: ensuring employees have the requisite technologies, securing connections, implementing team communication platforms, and setting clear

266. *See* Kelly, *supra* note 261 (discussing how JPMorgan has a work-from-home plan, but also send traders to from their New York City locations to offices in surrounding areas to conduct business); *see also* Davis, *supra* note 260 (discussing how JPMorgan Chase will toggle between remote and in-person work during the pandemic).

267. *See* Davis, *supra* note 260 (stating that banks having been "splitting up teams and traders amid different locations, and quarantining staff" in order to remain functioning during the pandemic).

268. *See id.* (discussing how banks are trying to have some employees work remotely to maintain safe operations during the pandemic).

269. *See id.* (explaining in further detail how regulatory plans for banking have developed protocols for workspace arrangements, i.e. how far apart employees should sit from each other, or how many can work remotely).

270. *See id.* (indicating that banks, like JPMorgan Chase, may need to develop resilient telecommuting policies for the future).

271. *See* Daniel Newman, *Distributed Companies, Work From Home, and the Technology Enabling the Change*, FORBES (Oct. 22, 2020, 10:14 AM), https://www.forbes.com/sites/danielnewman/2020/10/22/distributed-companies-work-from-home-and-the-technology-enabling-the-change/?sh=57d48af733bf [https://perma.cc/SGS4-TLYT] (discussing how companies need to invest in the right technologies for their employees working remotely).

272. *See* Boehm et al., *supra* note 88 ("[T]he recent COVID-19 pandemic has intensified the danger of cyberattack, across all industries. Changes in working conditions have made it harder for companies to maintain security. Large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services all present fresh openings, which cyberattackers have been quick to exploit.").

expectations on appropriate cyber-practices.[273] By investing capital into providing online services, banks can stay connected with consumers while still maintaining the quality of their services.[274]

The advantages for increased telework are clear.[275] While banks can realize a multitude of savings on office rent and supplies,[276] employee morale can be boosted as well.[277] Telework can even allow banks to dip into a more competitive and inclusive applicant pool since coming into the office is no longer essential.[278] The need to regularly come into the office can impose a significant hardship for some groups of people.[279] Eliminating the requirement for in-person work can offer more opportunities for people with disabilities and parents who seek employment in the banking industry.[280] Additionally, banks could benefit from increased corporate responsibility resulting from the telework model.[281] Remote employees will rely less on the need for

273. *See COVID-19 Work from Home Policy Best Practices*, AMTRUST FIN., https://amtrustfinancial.com/blog/small-busines/coronavirus-best-practices-work-from-home-policy [https://perma.cc/X6L5-N6RR] (last visited Feb. 6, 2021) (reporting on best practices for employees to follow while working remotely).

274. *See* Ryan Haar, *How the Pandemic Pushed a Generation of Americans to Discover the Perks (and Risks) of Online Banking*, TIME: NEXT ADVISOR (Sept. 25, 2020), https://time.com/nextadvisor/banking/how-the-pandemic-is-changing-banking/ [https://perma.cc/8LU9-DRGZ] (reporting that consumers will see the most added value in money reinvested in online banking services).

275. *See id.* (discussing advantages of mobile banking like convenience, easier financial planning, and less fees); *see also* Donna Fuscaldo, *Telecommuting: Should Your Company Make It Permanent?* BUS. NEWS DAILY (Sept. 16, 2020), https://www.businessnewsdaily.com/15817-should-telecommuting-be-permanent.html [https://perma.cc/958T-SSE9] (explaining that telework can allow employees to save money and work more productively).

276. *See* Fuscaldo, *supra* note 270 ("Telecommuting has proven to save money, boost morale and enhance the quality of life for many workers.").

277. *Id.*

278. *See id.* (discussing how remote employment enables companies to hire from a talented pool from all across the globe).

279. *See id.* ("[W]hen a physical office is out of the equation . . . it also means your business can hire people with disabilities who can't get to a physical office, single parents who are juggling families and work, and those who can't afford a car, train or bus to get to work.").

280. *See id.*

281. *See* Daniel Crow & Ariane Millot, *Working From Home Can Save Energy and Reduce Emissions. But How Much?* IEA (June 12, 2020), https://www.iea.org/commentaries/working-from-home-can-save-energy-and-reduce-emissions-but-how-much [https://perma.cc/QV9V-JRPW] (discussing how working from home could reduce employees' carbon footprint).

public transportation, thereby promoting environmental sustainability and reducing the bank's carbon footprint.[282]

Finally, policymakers need to consider the pragmatic effects of a remote workforce and amend existing privacy legislation in consideration of it.[283] The Telework Enhancement Act of 2010 ("Telework Act") is the most recent federal remote-work legislation,[284] which applies solely to executive agencies.[285] Under the Telework Act, federal agencies must (1) designate a telework managing officer (who is the primary contact point for telework matters),[286] (2) require all remote employees to complete telework training,[287] and (3) demand written agreements from all agencies setting forth their telework plan.[288] Furthermore, a push for new telework legislation has resurged in the form of the Pandemic Federal Telework Act ("Pandemic Telework Act"),[289] which, if passed, would require all federal agencies to maximize telework and expand the number of employees required to telework for the duration of COVID-19.[290] The expansion of telework would remain in effect until the COVID-19 public health emergency ends.[291] While the Telework Act and Pandemic Telework Act are aimed solely at federal employees, telework is more common in the private sector.[292] Thus, a comprehensive

282. *See id.* ("Our analysis shows that for people who commute by car, working from home is likely to reduce their carbon dioxide (CO2) footprint if their journey to work is greater than about 6 kilometers. However, for short car commutes or those done by public transport, working from home could increase CO2 emissions due to extra residential energy consumption.").

283. *See* Telework Enhancement Act of 2010, Public L. No. 111-292 12 Stat. 3165 (2010) (currently, the most recent legislation relating to telework) (currently, the most recent legislation relating to telework).

284. *Id.*

285. *Id.*

286. *Id.* § 6505.

287. *Id.* § 6503.

288. *Id.* § 6502–03.

289. Pandemic Federal Telework Act of 2020, S. 4518, 116th Cong. (proposed Aug. 10, 2020).

290. *Id.*

291. *See* Jessie Bur, *Maximum Federal Telework Gets a Second Senate Push*, FED. TIMES (Aug. 10, 2020), https://www.federaltimes.com/federal-oversight/congress/2020/08/10/maximum-federal-telework-gets-a-second-senate-push/ [https://perma.cc/9VF5-MVNF] (reporting that about 7% of the private sector teleworks compared to 4% in the public sector).

292. *See* Drew Desilver, *Before the Coronavirus, Telework Was an Optional Benefit, Mostly for the Affluent Few*, PEW RES. CTR. (Mar. 20, 2020), https://www.pewresearch.org/fact-tank/2020/03/20/before-the-coronavirus-telework-was-an-optional-benefit-mostly-for-the-affluent-few/ [https://perma.cc/9A82-B49D] ("Telework

federal telework act—covering both public and private employment sectors—could provide a framework for companies pursuing a permanent remote workforce in the future.[293]

Ensuring the safety and soundness of consumer financial data necessitates regulatory oversight of remote work.[294] Key provisions proposed in the Pandemic Telework Act would benefit from inclusion in a comprehensive federal telework act.[295] Such provisions include a determination of precisely which employees are telework-eligible,[296] and an implementation of mandatory telework training for supervisors and managers.[297] Given that many employees were not prepared to make the remote-work transition at the onset of the pandemic,[298] understanding which bank employees will telework is necessary for ensuring that these employees will be well equipped. While some employees were less inclined to follow safe data practices at home,[299] a federal telework act could provide guidance on what behaviors are permitted and prohibited. Because the financial services sector faces specific challenges pertaining to the protection of sensitive consumer data, oversight to ensure

---

is more common in the private sector than in state and local governments: About 7% of private-industry workers have access to it, versus 4% of state and local workers.").

293. Financial services companies have largely transitioned to a remote workforce since the pandemic began, and many companies have announced permanent work-from-home positions. *See, e.g.*, Bond, *supra* note 222 (reporting that Facebook "plans to begin 'aggressively' hiring remote workers, and it will soon allow some current employees to apply to work remotely on a permanent basis"); Brownlee, *supra* note 221 ("Recent announcements that virtually all Twitter and Square employees will have the option to work from home forever sent shock waves through business communities. . . . On the heels of surprisingly successful work from home experiences, survey data clearly suggest a momentum towards expanded work from home policies going forward.").

294. *See* George Mutune, *Work from Home Cyber Risks*, CYBER EXPERTS, https://cyberexperts.com/work-from-home-cyber-risks%EF%BB%BF/ [https://perma.cc/QJ2A-TF8Z] (last visited Jan. 5, 2021) (detailing risks of remote work environments).

295. *See id.* ("It is therefore necessary for every organization to be familiar with the different types of risks associated with remote working.")

296. Pandemic Federal Telework Act of 2020, § 2(b)(1)(A), S. 4518, 116th Cong. (proposed Aug. 10, 2020).

297. *Id.* § 4(3).

298. *See* Westfall, *supra* note 228 ("[M]ost workers are still unprepared for the challenges of working from home.").

299. *See Half of Employees Abandon Safe Data Practices*, *supra* note 230 ("A new report from email security firm Tessian looks at the state of data loss in organizations and reveals that *nearly half of employees (48%) are less likely to follow safe data practices when working from home*.") (emphasis added); *see also Going Digital*, *supra* note 247 ("[B]anking in the digital age requires a drastic, profound reset of how banking staff reacts to customer needs.").

employees are adhering to good cyber-risk management policies is critical.[300] Moreover, a federal telework act could provide civil penalties for non-compliance with safe data practices. If widespread telework is to continue then guidelines are necessary.

## VII. CONCLUSION

The financial services industry is overdue for a digital shakeup, and the security measures banks take in protecting consumer data need to be updated.[301] Massive breaches like Equifax and Capital One, along with the recent breaches seen during the pandemic, confirm the great length cybercriminals will go to in order to steal personal information.[302] As companies implement permanent work-from-home options, the financial services sector needs to be ready for a "new normal" in a post-pandemic world.[303] The reimagined financial industry should include full digitalization of the banking industry, comprehensive work-from-home plans, and amendments to existing privacy legislation to accommodate an increasingly remote workforce. Brick-and-mortar banks are becoming a thing of the past, and digital banks are on the rise. To survive, the industry must adapt.

ANNA-NICOLE C. COOKE*

300. *See What Are the Benefits and Challenges of Telework in Communication Technologies and Financial Services?* INT'L LAB. ORG. (Nov. 10, 2016), https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_534548/lang--en/index.htm [https://perma.cc/S8D5-Z2VK] (stating that there are challenges to remote work, including the need to protect consumer data).

301. *See* Mutune, *supra* note 294 (explaining the challenges of a work-from-home environment).

302. *See, e.g.,* Wack, *supra* note 49 (disclosing the details of Capital One's settlement with the Office of the Comptroller of the Currency); *Frequently Asked Questions*, *supra* note 96 (explaining what led to the 2019 data breach and the impact its had on consumers); *Equifax to Pay $575 Millio*n, *supra* note 47; Popper, *supra* note 196 (examining how cybercriminals have been targeting recipients of stimulus payments to help blunt the economic fallout of COVID-19); McKnight, *supra* note 210; Kundaliya, *supra* note 211 (detailing a data breach affecting applicants of the Paycheck Protection Program under Bank of America).

303. *See* Brownlee, *supra* note 221 ("On the heels of surprisingly successful work from home experiences, survey data clearly suggest a momentum towards expanded work from home policies going forward.").

* I would like to thank my mother and Colin LaPrade for their support and encouragement throughout the process of writing this Note. Additionally, I am incredibly grateful to Professor Lissa Broome, Katherine Franck, Lauren Davis, Thomas Walls, Ricky Willi, the rest of the editorial board, and the staff members of the North Carolina Banking Institute for their guidance and comments throughout the publication process.