Exhibit A

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

IN RE: EVOLVE BANK & TRUST CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to: All Cases.	2:24-md-03127-SHL-cgc

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Samantha Walker, Steven Mason, Tracy E. Starling, Terrance Pruitt, Duncan Meadows, Zachary Grisack, Christina Fava, Laura Robinson, Jo Joaquim, Nicole Petersen, Mark D. Van Nostrand, Sharyn Jackson, Evin Jason Shefa, and Lisa Adewole ("Plaintiffs"), bring this Consolidated Class Action Complaint on behalf of themselves and all others similarly situated ("Class Members" or "proposed Class Members"), against Defendant Evolve Bank and Trust ("Defendant" or "Evolve"). In support Plaintiffs allege as follows:

NATURE OF THE ACTION

1. This class action lawsuit arises out of Evolve's failure to implement reasonable and industry standard data security practices to properly secure and safeguard Plaintiffs' and the proposed Class Members' sensitive personally identifiable information ("PII"), which Evolve acquired and stored as part of its business relationship with various financial technology companies.

2. Defendant's data security failures resulted in the unauthorized access and theft of Plaintiffs' and Class Members' PII in a targeted cyberattack on Defendant's information systems or about June 18, 2024 (the "Data Breach").[1]

[1] *Cybersecurity Incident*, EVOLVE BANK & TRUST (last updated Aug. 27, 2024), https://www.getevolved.com/about/news/cybersecurity-incident/.

3. According to Defendant, the PII compromised in the Data Breach includes full names, Social Security numbers, dates of birth, financial account information, contact information, and other financial information.[2]

4. Defendant is a national financial services institution recognized as a global leader in the payments and banking-as-a-service ("BaaS") industry.[3] Defendant offers various products, including deposit accounts and payment processing services, to financial technology companies that in turn offer various financial products and services to consumers, either directly or through partnership with other entities.

5. Defendant knew or should have known its information systems were vulnerable prior to the Data Breach. On June 11, 2024, just days before the Data Breach, the Federal Reserve Board issued an enforcement action against Evolve for deficiencies in its risk management, anti-money laundering, and consumer compliance practices.[4] Though public filings do not make clear the failures identified by the Federal Reserve, the June 11, 2024 Order specifically required Defendant to "submit a written plan . . . including timetables, to correct the information technology and information security deficiencies identified in [examination reports completed by the Federal Reserve in August 2023 and January 2024]."[5]

6. Although the Federal Reserve Order was issued in 2024, the underlying

[2] *Id.*
[3] *Who We Are*, EVOLVE BANK & TRUST, https://www.getevolved.com/openbanking/who-we-are/ (last accessed Jan. 21, 2025).
[4] *In the Matter of Evolve Bancorp Inc. and Evolve Bank & Trust*, Cease and Desist Order Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, Dkt. Nos. 24-012-B-HC & 24-012-B-SM (June 11, 2024), https://www.federalreserve.gov/newsevents/pressreleases/files/enf20240614a1.pdf.
[5] *Id.* at 10, ¶ 6.

examinations were conducted in 2023.[6]

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect the highly sensitive PII in its custody.

8. The mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure PII from those risks left that property in a dangerous condition.

9. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequate robust computer systems and security practices to safeguard Plaintiffs' and Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

10. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed Plaintiffs' and Class Members' PII. Had it properly monitored its systems, Defendant would have discovered the intrusion sooner rather than allowing

[6] Bd. of Governors of the Fed. Res. Sys., Press Release: *Federal Reserve Board issues an enforcement action against Evolve Bancorp, Inc. and Evolve Bank & Trust for deficiencies in the bank's anti-money laundering, risk management, and consumer compliance programs*, (June 14, 2024), https://www.federalreserve.gov/newsevents/pressreleases/enforcement20240614a.htm ("Examinations conducted in 2023 found that Evolve engaged in unsafe and unsound banking practices by failing to have in place an effective risk management framework for [its] partnerships [with various financial technology companies]. In addition, Evolve did not maintain an effective risk management program or controls sufficient to comply with anti-money laundering laws and laws protecting consumers.").

cybercriminals a period of unimpeded access to Plaintiffs' and Class Members' PII.

11. If Defendant had implemented reasonable logging, monitoring, and alerting systems, it would have known about the malicious activity soon enough to enable it to stop the attack before the cybercriminals had time to identify digital assets, stage them for exfiltration, and then exfiltrate those assets without being caught.

12. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves.

13. Because of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their financial accounts to guard against fraud and identity theft. Because of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages.

14. The risk of future fraud and identity theft is not speculative or hypothetical but is impending and has materialized. There is evidence that Plaintiffs' and Class Members' PII was targeted and accessed in the Data Breach, and that it has already been misused and published on the Dark Web. The data stolen in the Data Breach includes all the necessary ingredients to allow cybercriminals to perpetrate financial and identity fraud, even without having to use "Fullz packages"[7] or otherwise buy additional information.

[7] Cybercriminals are known to piece together bits and pieces of compromised PII to develop "Fullz" packages. With Fullz packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data, with an astonishingly complete scope and degree of accuracy, to assemble complete dossiers on individuals. As a rule of thumb, the more information cybercriminals have on a victim, the more money they are able make using those credentials. Fullz packages are usually pricier than standard credit card

15. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts include and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

16. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual fraud and identity theft; (d) loss of time incurred due to actual fraud and identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collected and maintained.

17. Through this Complaint, Plaintiffs pursue legal redress for these harms on behalf

---

credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/.

of themselves and all similarly situated individuals whose PII was compromised in the Data Breach.

18. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

19. Plaintiff Samantha Walker is an adult individual and is a citizen of Jonesboro, Arkansas, where she intends to remain.

20. Plaintiff Steven Mason is an adult individual and a citizen of Shelbyville, Tennessee, where he intends to remain.

21. Plaintiff Tracy E. Starling is an adult individual and is a citizen of Smyrna, Georgia, where she intends to remain.

22. Plaintiff Terrance Pruitt is an adult individual and is a citizen of Southaven, Mississippi, where he intends to remain.

23. Plaintiff Duncan Meadows is an adult individual and is a citizen of San Marcos, California, where he intends to remain.

24. Plaintiff Zachary Grisack is an adult individual and is a citizen of Oroville, California, where he intends to remain.

25. Plaintiff Christina Fava is an adult individual and is a citizen of Las Vegas, Nevada, where she intends to remain.

26. Plaintiff Laura Robinson is an adult individual and is a citizen of Irvine, California, where she intends to remain.

27. Plaintiff Jo Joaquim is an adult individual and is a citizen of Hartford, Connecticut, where he intends to remain.

28. Plaintiff Nicole Petersen is an adult individual and is a citizen of Papillion, New England, where she intends to remain.

29. Plaintiff Mark D. Van Nostrand is an adult individual and is a citizen of Piedmont, Oklahoma, where he intends to remain.

30. Plaintiff Sharyn Jackson is an adult individual and is a citizen of Philadelphia, Pennsylvania where she intends to remain.

31. Plaintiff Evin Jason Shefa is an adult individual and is a citizen of Palm Desert, California, where he intends to remain.

32. Plaintiff Lisa Adewole is an adult individual and is a citizen of Austin, Texas, where she intends to remain.

33. Defendant Evolve is a bank headquartered in Memphis, Tennessee, that does significant business with FinTech and acts as the bank supporting their various services.

JURISDICTION AND VENUE

34. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenship from Defendant, including Plaintiffs. Indeed, the Class likely includes millions of individuals, and the some of the named Plaintiffs above are from states diverse from Defendant's citizenship.

35. This Court has personal jurisdiction over Defendants because their headquarters is

in Memphis, Tennessee.[8]

36. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiffs' and Class Members' PII in this District, and has caused harm to Plaintiffs and Class Members in this District.

FACTUAL BACKGROUND

37. Plaintiffs and Class Members are customers of Defendant who use Defendant's banking services, including through third-party financial technology companies ("FinTech companies").

38. When opening an account with Defendant or its partners, Plaintiffs and Class Members were required to provide their sensitive and personal information, including financial information, contact information, and Social Security numbers.

39. Indeed, the notification emails that Plaintiffs have received confirmed that Defendant collected and stored their financial information and Social Security numbers, among other valuable PII.

40. Notwithstanding its duty to implement reasonable cybersecurity, Defendant failed to implement sufficient logging, monitoring, and alerting systems that would have allowed it to detect that it was being attacked in a timely manner so that it could prevent the exfiltration of Plaintiffs' and the proposed Class Members' information, including tools sufficient to identify when large amounts of data were being downloaded unauthorizedly.

41. Yet, Defendant did not know it was being attacked until May 29, 2024, when it

[8] Contact Us, EVOLVE BANK & TRUST, https://www.getevolved.com/contact/contact-us (last accessed Jan. 21, 2025).

noticed that some of its systems were no longer functioning as expected.

42. At first, Defendant believed the failures to be related to hardware issues, rather than a cybersecurity attack.

43. On information and belief, and because it is the modus operandi of cybercriminals, the hackers had already performed reconnaissance activities, staged data, and exfiltrated the stolen data before Defendant even knew that the IT outages were due to a cyberattack. The failure to understand what was happening is clear evidence of Evolve's failure to implement reasonable tools to monitor the events happening in its information systems.

44. Indeed, the so-called hardware issues on Defendant's information systems were the result of the hackers' ransomware attack, which is only performed after the hackers have completed downloading the stolen data.

45. At all relevant times, Defendant knew it was storing Plaintiffs' and Class Members' PII, and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

46. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, especially given that Data Breaches have, unfortunately, become ubiquitous.

47. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers can easily sell stolen data because of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[9]

[9] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company.

48. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[10]

49. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[11]

50. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' customers especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

51. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[12]

---

[10] Identity Theft Res. Ctr., *Data Breach Reports: 2019 End of Year Report*, at 2, https://notified.idtheftcenter.org/s/resource#annualReportSection.

[11] Insurance Information Inst., *Facts + Statistics: Identity theft and cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

[12] U.S. Gov't Accountability Office, *Report to Congressional Requesters, Personal Information*, (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

52. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

53. Defendant agreed to and undertook legal duties to maintain the PII entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Under state and federal law, businesses like Defendant have a duty to protect their clients' current and former customers' PII and to notify them about breaches.

54. The PII held by Defendant in its computer system and network included the highly sensitive PII of Plaintiffs and Class Members.

55. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, to protect Plaintiffs' and Class Members' PII.

56. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs' and Class Members' significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to: (1) closely monitor their bank statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other

communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

57. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendant's conduct. Further, the value of Plaintiffs' and Class Members' PII has been diminished by its exposure in the Data Breach.

58. As a result of Defendant's failures, Plaintiffs and Class Members are at a substantially increased risk of suffering identity theft, fraud, or other misuse of their PII.

59. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[13]

60. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[14]

61. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect Plaintiffs' and Class Members' PII.

---

[13] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, SECURITY AWARENESS TRAINING BLOG, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

[14] *See* Identity Theft Res. Ctr., https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis.

62. Because of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

63. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

64. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

65. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

66. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[15] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on

[15] *What Is the Dark Web?*, Experian, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[16] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

67. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal information like the PII at issue here.[17] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[18] As Microsoft warns: "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[19]

68. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls

[16] *Id.*
[17] *What is the Dark Web?* – Microsoft 365, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[18] *Id.*; EXPERIAN, *What Is the Dark Web?*, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[19] *Supra* n.13.

> from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

69. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

70. Even then, a new Social Security number may not be effective, as the "credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

71. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[22]

72. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime

---

[20] Social Security Admin., *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.

[21] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[22] Social Security Admin., *Identity Theft and Your Social Security Number*, at 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[23]

73. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[24] Defendant did not rapidly report to Plaintiffs and the Class that their PII had been stolen.

74. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

75. In addition to out-of-pocket expenses that can exceed thousands of dollars, and the emotional toll identity theft can take, victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

76. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[25]

77. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data

---

[23] *See* Fed. Bureau of Investigations, *2019 Internet Crime Report Released*, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[24] *Id.*
[25] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[26]

78. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

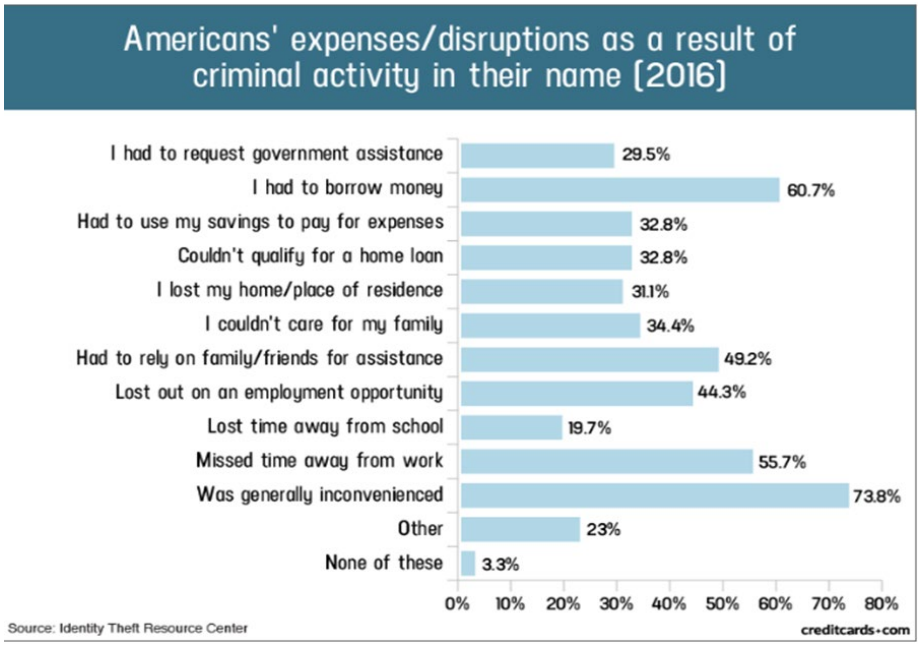
79. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm, but the resource and asset of time has been lost.

80. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and

[26] *See generally*, Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

filing police reports, which may take years to discover and detect.

81. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[27]



82. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their

[27] Jason Steele, *Credit Card and ID Theft Statistics*, (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[28] *See* U.S. Gov't Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, p. 2 (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

83. PII is a valuable property right.[30] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

84. PII can sell for as much as $363 per record according to the Infosec Institute.[31]

85. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[32] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33, 34] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[35]

86. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be

---

[29] *See* Fed. Trade Comm'n, *Steps*, https://www.identitytheft.gov/Steps.
[30] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[31] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[32] David Lazarus, *Column: Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[33] https://datacoup.com/.
[34] https://digi.me/what-is-digime/.
[35] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

available and holds significant value for the threat actors.

87. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for credit monitoring and identity protection services, as opposed to automatically enrolling all victims of this Data Breach.[36]

88. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes (e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims).

89. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[37] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

---

[36] *Id*.

[37] *See* Jesse Damiani, *Your Social Security Number Costs $4 On the Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

91. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

92. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from this Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

93. Moreover, Plaintiffs and Class Members have an interest in ensuring that PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

94. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, they have suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continued publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII;

h. Significant emotional and mental anguish, stress, and anxiety caused by the uncertainty of the financial future because of Defendant's negligence, which resulted in their highly sensitive PII falling into the hands of cybercriminals adept at exploiting such information for their nefarious financial fraud and identity theft objectives; and

i. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

95. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their PII in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

96. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

97. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

98. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects

of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Visiting banks to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending significant time and effort disputing fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

99. In addition, Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in similar cases.

100. Plaintiffs and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy

whatsoever.

101. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII. Early notification helps a victim of a Data Breach mitigate their injuries, and conversely, delayed notification causes more harm and increases the risk of identity theft.

PLAINTIFFS' EXPERIENCES

Plaintiff Samantha Walker

102. Plaintiff Walker received an email from PrizePool on June 26, 2024, informing her that the information she shared with PrizePool had been compromised as part of the Evolve Bank & Trust Data Breach.

103. On July 3, 2024, Plaintiff received an update email from PrizePool informing here that her name, date of birth, Social Security number, address, phone number, bank account number, linked bank account number, and debit card number were likely compromised in the Evolve Data Breach.

104. Similarly, Plaintiff Walker received a notification email from Juno informing her that the information she shared with it was also affected by the Evolve Bank & Trust Data Breach, including her Social Security number, bank account number, and her contact information.

105. The email noted that the same was true for many other FinTech companies, including Affirm, Mercury, Plaid, Bilt, Wise, Branch, and more.

106. Plaintiff Walker values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

107. Plaintiff Walker has been injured in several ways, including by the damage to and

diminution in value of her PII—a form of intangible property that Plaintiff entrusted to Evolve. Her information has inherent value that Plaintiff Walker was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

108. The Data Breach has also caused Plaintiff Walker to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals.

109. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Walker to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred. Her time, which has been lost forever and cannot be recaptured.

110. The present and substantial risk of imminent harm and loss of privacy have both caused Plaintiff Walker to suffer stress, fear, and anxiety.

111. Plaintiff Walker has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Steven Mason

112. On July 24, 2024, Mr. Mason received a notification email directly from Evolve informing him that his information had been stolen in the Data Breach, including his name, contact information, Evolve account number, Social Security number, and date of birth.

113. Because Plaintiff Mason's sensitive PII is now in the hands of cybercriminals, he has suffered significant stress and anxiety over his future financial health and the uncertainty of how he can protect himself from such further harm.

114. Plaintiff Mason has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity.

115. Furthermore, Mr. Mason has experienced a drop in his credit score because of the Data Breach due to hard inquiries on his credit score that he never authorized from at least two financial institutions.

116. Since the Data Breach, Mr. Mason has also been harassed with a substantial increase in spam and phishing messages.

117. Still further, Mr. Mason is also a customer of the FinTech company Dave. After the Data Breach, he lost all access to his Dave account. When he called to attempt to regain access to his account, he was informed that he would need to provide proof of his identity because of unusual activity on the account. After sending the requested information and proof, he still has not heard back from Dave or regained control over his account, which was apparently the successful target of identity thieves.

118. Still further, Mr. Mason has been locked out of his my.fico.com account, which, given his experience with his Dave account, is believed to be because of unlawful access attempts.

119. Plaintiff Mason values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

120. Plaintiff Mason has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiff Mason entrusted to Evolve. This information has inherent value that Plaintiff Mason was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

121. The Data Breach has also caused Plaintiff Mason to suffer imminent and impending

injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for his lifetime resulting from his PII being placed in the hands of criminals.

122. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Mason to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured.

123. The present and substantial risk of imminent harm and loss of privacy have both caused Plaintiff Mason to suffer stress, fear, and anxiety.

124. Plaintiff Mason has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Tracy E. Starling

125. On or about July 26, 2024, Plaintiff Starling received a notification email directly from Evolve informing her that her information had been stolen in the Data Breach.

126. Plaintiff Starling has spent significant time responding to Evolve's Data Breach, including by reviewing her credit and account statements for fraudulent activity. Plaintiff Starling has already experienced fraud and identity theft since the Evolve Data Breach, experiencing attempted fraudulent activity on her credit card by someone Hong Kong, and frequently receives notifications that someone is attempting to access her Shopify account. Moreover, payday loans that Plaintiff did not take out have appeared on her credit reports.

127. Since the Data Breach, Plaintiff Starling has also been harassed with a substantial increase in spam and phishing messages.

128. Plaintiff Starling values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

129. Plaintiff Starling has been injured in several ways, including by the damage to and diminution in value of her PII—a form of intangible property that Plaintiff Starling entrusted to Evolve. This information has inherent value that Plaintiff Starling was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

130. The Data Breach has also caused Plaintiff Starling to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Starling has already experienced such fraud, theft, and misuse of her PII.

131. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Starling to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time has been lost forever and cannot be recaptured.

132. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Starling to suffer stress, fear, and anxiety.

133. Plaintiff Starling has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Terrance Pruitt

134. In August of 2024, Plaintiff Pruitt received a notification email directly from Evolve informing him that his information had been stolen in the Data Breach.

135. Plaintiff Pruitt has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity and closing his Evolve accounts. Plaintiff Pruitt has already experienced fraud and identity theft since the Evolve Data Breach, with four loans that he did not take out appearing on his credit report and experiencing fraudulent attempts to apply for a Discover credit card and open a Fingerhut credit account in his name. Moreover, Plaintiff Pruitt has received alerts that his information is on the dark web.

136. Since the Data Breach, Plaintiff Pruitt has also been harassed with a substantial increase in spam and phishing messages.

137. Plaintiff Pruitt values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

138. Plaintiff Pruitt has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiff Pruitt entrusted to Evolve. This information has inherent value that Plaintiff Pruitt was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

139. The Data Breach has also caused Plaintiff Pruitt to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for his lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Pruitt has already experienced such fraud, theft, and misuse of his PII.

140. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Pruitt to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time, which has been lost forever and cannot be recaptured.

141. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Pruitt to suffer stress, fear, and anxiety.

142. Plaintiff Pruitt has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Duncan Meadows

143. Plaintiff Meadows started on online business using the e-commerce platform Shopify. As part of that process, Shopify partners with Defendant to provide banking related services for Shopify businesses. Plaintiff Meadows elected to utilize that banking partnership as part of his business and provided Defendant his PII, including but not limited to, his Social Security number, date of birth and address to receive banking products and services from Defendant.

144. On or about June 27, 2024, Plaintiff Meadows received an email message from Shopify notifying him that his PII, which had been provided to Defendant, had been improperly accessed and taken by unauthorized third parties.

145. Plaintiff Meadows has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity. Plaintiff Meadows has already experienced fraud and identity theft since the Evolve Data Breach, as someone fraudulently attempted to take out a mortgage in his name, and Plaintiff Meadows received four

hard inquiries on his credit report around the time of the Data Breach. Additionally, in March of 2024, Plaintiff Meadows experienced a fraudulent attempt to take out a student loan in his name.

146. Since the Data Breach, Plaintiff Meadows has also been harassed with a substantial increase in spam and phishing messages.

147. Plaintiff Meadows values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

148. Plaintiff Meadows has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiffs entrusted to Evolve. This information has inherent value that Plaintiff Meadows was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

149. The Data Breach has also caused Plaintiff Meadows to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for his lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Meadows has already experienced such fraud, theft, and misuse of his PII.

150. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Meadows to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time, which has been lost forever and cannot be recaptured.

151. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Meadows to suffer stress, fear, and anxiety.

152. Plaintiff Meadows has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Zachary Grisack

153. Plaintiff Grisack received a notification email directly from Evolve informing him that his information had been stolen in the Data Breach. Because Plaintiff Grisack's sensitive PII is now in the hands of cybercriminals, he has suffered significant stress and anxiety over his future financial health and the uncertainty of how he can protect himself from such further harm.

154. Plaintiff Grisack has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity. Plaintiff Grisack has already had two fraudulent American Express cards opened in his name since the Evolve Data Breach. Moreover, Plaintiff Grisack has received alerts that his information is on the dark web.

155. Since the Data Breach, Plaintiff Grisack has also been harassed with a substantial increase in spam and phishing messages.

156. Plaintiff Grisack values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

157. Plaintiff Grisack has been injured in a number of ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiffs entrusted to Evolve. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

158. The Data Breach has also caused Plaintiff Grisack to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity

theft, and misuse for his lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Grisack has already experienced such fraud, theft, and misuse of his PII.

159. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Grisack to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time, which has been lost forever and cannot be recaptured.

160. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Grisack to suffer stress, fear, and anxiety.

161. Plaintiff Grisack has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Christina Fava

162. Plaintiff Fava received a notification email and a letter via regular mail directly from Evolve informing her that her information had been stolen in the Data Breach.

163. Plaintiff Fava has spent significant time responding to Evolve's Data Breach, including by reviewing her credit and account statements for fraudulent activity. Plaintiff Fava has already experienced fraud and identity theft since the Evolve Data Breach, having to cancel her credit card due to suspicious activity, and US Bank closed Plaintiff Fava's checking and savings accounts after final review for suspicious activity. Additionally, Plaintiff Fava was forced to dispute a fraudulent Amex savings account that was opened in Plaintiff's name and has five current disputes due to fraudulent charges.

164. Since the Data Breach, Plaintiff Fava has also been harassed with a substantial increase in spam and phishing messages. These calls became so frequent that Plaintiff Fava got in trouble at work due to the volume of calls that she was receiving.

165. Plaintiff Fava values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

166. Plaintiff Fava has been injured in several ways, including by the damage to and diminution in value of her PII—a form of intangible property that Plaintiffs entrusted to Evolve. This information has inherent value that Plaintiff Fava was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

167. The Data Breach has also caused Plaintiff Fava to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Fava has already experienced such fraud, theft, and misuse of her PII.

168. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Fava to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time has been lost forever and cannot be recaptured.

169. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Fava to suffer stress, fear, and anxiety.

170. Plaintiff Fava has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and

safeguarded from future breaches.

Plaintiff Laura Robinson

171. Plaintiff Robinson received a notification email and a letter via regular mail directly from Evolve informing her that her information had been stolen in the Data Breach.

172. Plaintiff Robinson has spent significant time responding to Evolve's Data Breach, including by reviewing her credit and account statements for fraudulent activity. Plaintiff Robinson has already experienced fraud and identity theft since the Evolve Data Breach, including having her US Bank account closed due to unauthorized charges in or around July of 2024.

173. Since the Data Breach, Plaintiff Robinson has also been harassed with a substantial increase in spam and phishing messages.

174. Plaintiff Robinson values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

175. Plaintiff Robinson has been injured in several ways, including by the damage to and diminution in value of her PII—a form of intangible property that Plaintiff Robinson entrusted to Evolve. This information has inherent value that Plaintiff Robinson was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

176. The Data Breach has also caused Plaintiff Robinson to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Robinson has already experienced such fraud, theft, and misuse of her PII.

177. In addition to the increased risk and the actual harm suffered, the Data Breach has

caused Plaintiff Robinson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time has been lost forever and cannot be recaptured.

178. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Robinson to suffer stress, fear, and anxiety.

179. Plaintiff Robinson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Jo Joaquim

180. On June 28, 2024, Plaintiff Joaquim received an email from Wise, informing him that some of his information had been compromised as part of the Evolve Data Breach.

181. On July 25, 2024, Plaintiff Joaquim received a notification email directly from Evolve informing him that his information had been stolen in the Data Breach, including his name, contact information, Evolve account number, Social Security number, and date of birth.

182. Because Plaintiff Joaquim's sensitive PII is now in the hands of cybercriminals, he has suffered significant stress and anxiety over his future financial health and the uncertainty of how he can protect himself from such further harm.

183. Plaintiff Joaquim has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity. Plaintiff Joaquim has already suffered fraud and identity theft through a fraudulent attempt to take out a $240,000 home loan through American Funding around February 2024. Around this same time, Plaintiff Joaquim also received a notice from West Lake Bank that he was denied a car loan that he did not

apply for.

184. Since the Data Breach, Plaintiff Joaquim has also been harassed with a substantial increase in spam and phishing messages.

185. Plaintiff Joaquim values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

186. Plaintiff Joaquim has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiff Joaquim entrusted to Evolve. This information has inherent value that Plaintiff Joaquim was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

187. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for his lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff has already experienced such fraud, theft, and misuse of his PII.

188. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Joaquim to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time, which has been lost forever and cannot be recaptured.

189. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Joaquim to suffer stress, fear, and anxiety.

190. Plaintiff Joaquim has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and

safeguarded from future breaches.

Plaintiff Nicole Petersen

191. Plaintiff Peterson received a notification email directly from Evolve informing her that her information had been stolen in the Data Breach.

192. Plaintiff Peterson has spent significant time responding to Evolve's Data Breach, including by reviewing her credit and account statements for fraudulent activity. Plaintiff Peterson has already experienced fraud and identity theft since the Evolve Data Breach, including unauthorized charges on two of her cards: a $60 charge in New Jersey that her bank detected and shut down her card, and a notification regarding $50 and $2 charges being attempted internationally, which eventually led to that card being shut down as well. Additionally, Plaintiff Peterson has received alerts that her information is on the dark web.

193. Since the Data Breach, Plaintiff Peterson has also been harassed with a substantial increase in spam and phishing messages.

194. Plaintiff Peterson values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

195. Plaintiff Peterson has been injured in several ways, including by the damage to and diminution in value of her PII—a form of intangible property that Plaintiff Peterson entrusted to Evolve. This information has inherent value that Plaintiff Peterson was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

196. The Data Breach has also caused Plaintiff Peterson to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals.

Indeed, as noted above, Plaintiff Peterson has already experienced such fraud, theft, and misuse of her PII.

197. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Peterson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time has been lost forever and cannot be recaptured.

198. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Peterson to suffer stress, fear, and anxiety.

199. Plaintiff Peterson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Mark D. Van Nostrand

200. Plaintiff Van Nostrand received a notification email directly from Evolve Bank & Trust informing him that his information had been stolen in the Data Breach. Because Plaintiff Van Nostrand's sensitive PII is now in the hands of cybercriminals, he has suffered significant stress and anxiety over his future financial health and the uncertainty of how he can protect himself from such further harm.

201. Plaintiff Van Nostrand has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity. Plaintiff Van Nostrand has already experienced fraud and identity theft, having received notices from Best Buy and Affirm that someone attempted to open accounts in his name. Plaintiff Van Nostrand has been unable to open another account because he can't verify his identity, which has damaged his

credit score.

202. Since the Data Breach, Plaintiff Van Nostrand has also been harassed with a substantial increase in spam and phishing messages.

203. Plaintiff Van Nostrand values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

204. Plaintiff Van Nostrand has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiff Van Nostrand entrusted to Evolve. This information has inherent value that Plaintiff Van Nostrand was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

205. The Data Breach has also caused Plaintiff Van Nostrand to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for his lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Van Nostrand has already experienced such fraud, theft, and misuse of his PII.

206. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Van Nostrand to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred, and resolving fraudulent activity. This time, which has been lost forever and cannot be recaptured.

207. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Van Nostrand to suffer stress, fear, and anxiety.

208. Plaintiff Van Nostrand has a continuing interest in ensuring that his PII, which,

upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Sharyn Jackson

209. Plaintiff Jackson received a notification letter directly from Evolve informing her that her information had been stolen in the Data Breach.

210. Plaintiff Jackson has spent significant time responding to Evolve's Data Breach, including by reviewing her credit and account statements for fraudulent activity. Plaintiff Jackson has already experienced fraud and identity theft since the Evolve Data Breach, including collection notices from electric companies for a service address in Houston, Texas, even though Plaintiff Jackson has never lived in any other state besides Pennsylvania. Plaintiff Jackson also had hard inquiries on her credit from Direct Energy, US retailers, and Green Mountain Energy,

211. Since the Data Breach, Plaintiff Jackson has also been harassed with a substantial increase in spam and phishing messages.

212. Plaintiff Jackson values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

213. Plaintiff Jackson has been injured in several ways, including by the damage to and diminution in value of her PII—a form of intangible property that Plaintiff Jackson entrusted to Evolve. This information has inherent value that Plaintiff Jackson was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

214. The Data Breach has also caused Plaintiff Jackson to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals.

Indeed, as noted above, Plaintiff Jackson has already experienced such fraud, theft, and misuse of her PII.

215. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Jackson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time has been lost forever and cannot be recaptured.

216. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Jackson to suffer stress, fear, and anxiety.

217. Plaintiff Jackson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Evin Jason Shefa

218. Plaintiff Shefa received a notification email directly from Evolve informing him that his information had been stolen in the Data Breach. Because Plaintiff Shefa's sensitive PII is now in the hands of cybercriminals, he has suffered significant stress and anxiety over his future financial health and the uncertainty of how he can protect himself from such further harm.

219. Plaintiff Shefa has spent significant time responding to Evolve's Data Breach, including by reviewing his credit and account statements for fraudulent activity. Plaintiff Shefa has already experienced fraud and identity theft, having experienced fraudulent charges for $80 on a credit card. Additionally, Plaintiff Shefa has received alerts that his information is on the dark web.

220. Since the Data Breach, Plaintiff Shefa has also been harassed with a substantial

increase in spam and phishing messages.

221. Plaintiff Shefa values his privacy and makes every reasonable effort to keep his personal information private, but he lost control over that privacy when Evolve allowed cybercriminals unfettered access to his data.

222. Plaintiff Shefa has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiff Shefa entrusted to Evolve. This information has inherent value that Plaintiff Shefa was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

223. The Data Breach has also caused Plaintiff Shefa to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for his lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Shefa has already experienced such fraud, theft, and misuse of his PII.

224. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Shefa to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred, and resolving fraudulent activity. This time, which has been lost forever and cannot be recaptured.

225. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Shefa to suffer stress, fear, and anxiety.

226. Plaintiff Shefa has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Lisa Adewole

227. On or about July 26, 2024, Plaintiff Adewole received a notification letter directly from Evolve informing her that her information had been stolen in the Data Breach.

228. Plaintiff Adewole has spent significant time responding to Evolve's Data Breach, including by reviewing her credit and account statements for fraudulent activity. Plaintiff Adewole has already experienced fraud and identity theft since the Evolve Data Breach, experiencing attempted fraudulent activity on her credit card and was forced to request a new card. Plaintiff Adewole has received alerts that her information is on the dark web and had to pay for credit monitoring at $25/month after the breach.

229. Since the Data Breach, Plaintiff Adewole has also been harassed with a substantial increase in spam and phishing messages.

230. Plaintiff Adewole values her privacy and makes every reasonable effort to keep her personal information private, but she lost control over that privacy when Evolve allowed cybercriminals unfettered access to her data.

231. Plaintiff Adewole has been injured in several ways, including by the damage to and diminution in value of his PII—a form of intangible property that Plaintiff Adewole entrusted to Evolve. This information has inherent value that Plaintiff Adewole was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

232. The Data Breach has also caused Plaintiff Adewole to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse for her lifetime resulting from her PII being placed in the hands of criminals. Indeed, as noted above, Plaintiff Adewole has already experienced such fraud, theft, and misuse of her PII.

233. In addition to the increased risk and the actual harm suffered, the Data Breach has

caused Plaintiff Adewole to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring accounts and credit reports to ensure no fraudulent activity has occurred and resolving fraudulent activity. This time has been lost forever and cannot be recaptured.

234. The present and substantial risk of imminent harm and loss of privacy has caused Plaintiff Adewole to suffer stress, fear, and anxiety.

235. Plaintiff Adewole has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS ALLEGATIONS

236. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following proposed Nationwide Class (the "Class") and state subclass ("Subclass"):

> **Nationwide Class:** All individuals in the U.S. whose PII was compromised in the Data Breach.
>
> **California Subclass:** All citizens of California whose PII was compromised in the Data Breach.

237. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

238. Plaintiffs reserve the right to modify or amend the definition of the proposed Class prior to moving for class certification.

239. **Numerosity.** The Class described above are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Though the exact size of the Class remains unknown, but it is believed to be in the millions.

240. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiffs and Class Members' PII;

c. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiffs' and Class Members' PII, and breached its duties thereby;

d. Whether Defendant breached its fiduciary duty to Plaintiffs and the Class.

e. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

f. Whether Plaintiffs and Class Members are entitled to restitution or disgorgement because of Defendant's wrongful conduct; and

g. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

241. **Typicality.** Plaintiffs' claims are typical of the claims of the Class Members. The

claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiffs and Class Members information was stored by Defendant's software, each having their PII obtained by an unauthorized third party.

242. **Adequacy of Representation.** Plaintiffs is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members they seek to represent; Plaintiffs has retained counsel competent and experienced in complex class action litigation; Plaintiffs intends to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

243. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant breached its common law and statutory duties to secure PII on its network server, then Plaintiffs and each Class Member suffered damages from the exposure of sensitive PII in the Data Breach.

244. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

245. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendant's records. The claims of Plaintiffs and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

246. Plaintiffs hereby repeat and reallege the foregoing allegations.

247. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

248. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

249. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

250. Defendant's duty also arose from Defendant's position as a financial institution and e-commerce cite. Defendant holds itself out as a trusted data collector, and thereby assumes a duty to reasonably protect its customers' employees' information. Indeed, Defendant, as a direct data collector, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members because of the Data Breach.

251. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and

compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its clients.

252. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

253. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including—as interpreted and enforced by the FTC—the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

254. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving the PII of its customers.

255. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

256. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

257. The harm that has occurred because of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

258. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class

Members have suffered injuries, including:

a. Privacy violations due to the disclosure of their private information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts, including the costs of credit monitoring;

c. Lowered credit scores from credit inquiries following fraudulent activities;

d. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

e. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals because of the disclosure of Plaintiffs' and the proposed Class Members' financial information and Social Security numbers being divulged to cybercriminals;

f. Damages to, and diminution in value of, their PII entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

g. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

h. The erosion of the essential and confidential relationship between

Defendant—as a banking provider—and Plaintiffs and Class Members as its clients' customers; and

i. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

259. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF THIRD-PARTY BENFICIARY CONTRACT
(On Behalf of Plaintiffs and the Class)

260. Plaintiffs hereby repeat and reallege the foregoing allegations.

261. Defendant entered contracts with its clients to provide services that explicitly or implicitly included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

262. Indeed, because such safeguards are required by industry standard and applicable statutory, common, and regulatory law, the implementation and maintenance of such safeguards is required to fulfill a parties' contractual obligations of good faith and fair dealing in their performance.

263. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their PII that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts. Indeed, the sole purpose of the contracts was to enable the provision of financial services to Plaintiffs and the proposed Class Members.

264. Defendant knew that if it were to breach these contracts with its clients, Plaintiffs and Class Members would be harmed.

265. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

266. As foreseen, Plaintiffs and the proposed Class Members were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII and the loss of control over how it was used and who had access to it.

267. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

268. Plaintiffs hereby repeat and reallege the foregoing allegations.

269. Plaintiffs bring this claim in the alternative—pursuant to Rule 8 of the Federal Rules of Civil Procedure—to their breach of third-party beneficiary contract claim above.

270. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their PII, which Defendant has made significant profit from. In exchange, Defendant should have provided adequate data security for Plaintiffs and Class Members, which was required by statutory, common, and regulatory law.

271. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their PII as a necessary part of their obtaining services at Defendant's bank. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the PII

of Plaintiffs and Class Members for business purposes.

272. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

273. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

274. Defendant, however, failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

275. Defendant would not be able to carry out an essential function of its regular business without the PII of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

276. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

277. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have allowed their PII to be provided to Defendant.

278. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and

Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

279. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

280. Plaintiffs and Class Members have no adequate remedy at law.

281. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

282. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

283. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and

Class Members overpaid for Defendant's services.

FOURTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
UNLAWFUL BUSINESS PRACTICE
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(By Plaintiffs Duncan Meadows, Zachary Grisack, Laura Robinson, Evin Jason Shefa, and on Behalf of the California Subclass)

284. Plaintiffs hereby repeat and reallege the foregoing allegations.

285. Plaintiffs bring this Count on their own behalf and on behalf of the California Subclass (the "Class" for the purposes of this Count).

286. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

287. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

288. Defendant stored the PII of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs' and the Class's PII secure so as to prevent the loss or misuse of that PII.

289. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure. However, Plaintiffs and the Class were entitled to assume, and did assume that Defendant had secured their PII. At no time were Plaintiffs and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

290. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and

exfiltration, theft, or disclosure of Plaintiffs' and the Class's nonencrypted and nonredacted PII.

291. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

292. Defendant's conduct was unlawful, in that it violated the CCPA.

293. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

294. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

295. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

296. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

297. Instead, Defendant made the PII of Plaintiffs and the Class accessible to scammers,

identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

298. As a result of those unlawful and unfair business practices, Plaintiffs and the Class suffered an injury-in-fact and have lost money or property.

299. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all the circumstances.

300. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

301. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

FIFTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code § 1798.80, *et seq*.
(By Plaintiffs Duncan Meadows, Zachary Grisack, Laura Robinson, Evin Jason Shefa, and on Behalf of the California Subclass)

302. Plaintiffs hereby repeat and reallege the foregoing allegations.

303. Plaintiffs brings this Count on their own behalf and on behalf of the California Subclass (the "Class" for the purposes of this Count).

304. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the

data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (*Id.*), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

305. The Data Breach constitutes a "breach of the security system" of Defendant.

306. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class.

307. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class, but waited approximately fourteen months to notify them. Fourteen months was an unreasonable delay under the circumstances.

308. Defendant's unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

309. Because Plaintiffs and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

310. Plaintiffs and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

SIXTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.150
(By Plaintiffs Duncan Meadows, Zachary Grisack, Laura Robinson, Evin Jason Shefa, and on Behalf of the California Subclass)

311. Plaintiffs hereby repeat and reallege the foregoing allegations.

312. Plaintiffs brings this Count on their behalf and on behalf of the California Subclass

(the "Class" for the purposes of this Count).

313. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the Class. As a direct and proximate result, Plaintiffs' and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

314. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

315. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiffs' and Class members' PII. Plaintiffs and Class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

316. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiffs believes such cure is not possible under these facts and circumstances—then Plaintiffs intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

317. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate

to the nature of the information so as to protect the personal information under the CCPA.

318. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the putative Class, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide to the Court

reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the PII of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps

affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: January 21, 2025

Respectfully Submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (BPR 23045)
Grayson Wells (BPR 039658)
Stranch, Jennings & Garvey, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801

gstranch@stranchlaw.com
gwells@stranchlaw.com

Lead Class Counsel

Gary M. Klinger
MILBERG COLEMAN BRYSON GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

Lynn A. Toops
Amina Thomas
COHEN & MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

Jeff Ostrow
KOPELOWITZ OSTROW, P.A.
1 W. Las Olas Boulevard, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Linda Nussbaum
NUSSBAUM LAW GROUP P.C.
1133 Avenues of the Americas, 31st Floor
New York, NY 10036
Tel: (917) 438-9102
lnussbaum@nussbaumpc.com

James J. Pizzirusso
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, DC 20006
Tel: (202) 540-7200
jpizzirusso@hausfeld.com

Scott Poynter
POYNTER LAW GROUP
4924 Kavanaugh Boulevard

Little Rock, AR 72207
Tel: (501) 812-3943
scott@poynterlawgroup.com

Members of the Class Counsel Executive Committee

Frank L. Watson, III
WATSON BURNS, PLLC
253 Adams Avenue
Memphis, TN 38104
Tel: (901) 529-7996
fwatson@watsonburns.com

Class Liaison Counsel

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was submitted via electronic mail and/or was electronically filed with the Clerk of the Clerk via the ECF System, which forwarded electronic notification of the filing to all counsel of record.

This the 21st day of January, 2025

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (BPR 23045)