Alex R. Straus (SBN 321366)
astraus@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
T: 917-471-1894
F: 865-522-0049

Attorneys for Plaintiff

[*Additional Attorneys Identified in Signature Block*]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MARSHALL GRIFFIN, on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. GEMINI TRUST COMPANY, LLC, and IRA FINANCIAL TRUST COMPANY, Defendants.	CASE NO. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Marshall Griffin ("Plaintiff"), on behalf of himself and all others similarly situated (the "Class Members"), brings this Class Action Complaint against Defendants Gemini Trust Company, LLC ("Gemini") and IRA Financial Trust Company ("IRA Financial") (collectively, the "Defendants"). The allegations in this Complaint are based on the personal knowledge of Plaintiff or upon information and belief and investigation of counsel.

NATURE OF CASE

1. This is a data breach class action brought on behalf of ***consumers whose retirement savings were stolen*** by cybercriminals in a massive cyber-attack at IRA Financial—one of a handful of firms that runs certain of its retirement account services through Gemini (a leading cryptocurrency exchange)—in or around February 2022 (the "Data Breach"). The Data Breach reportedly resulted in at least $36 million in crypto currency stolen from Class Members' individual retirement accounts ("IRAs"), including Plaintiff who lost 2 Bitcoins worth approximately $85,000.

2. Both IRA Financial and Gemini are placing the blame on each other. According to IRA Financial spokesperson Maria Stagliano, IRA Financial's investigation is primarily focused on security controls that IRA Financial claims weren't offered or available from Gemini. For its part, Gemini claims that its investigation found that the transactions it processed appeared to be "legitimate, authorized transactions."

3. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of actual monies, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Plaintiff's and Class Members' retirement savings—the most sacred monies for any person—were compromised, unlawfully accessed, and stolen due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Plaintiff's and Class Members' IRAs that they services, maintained and/or held in trust.

6. Upon information and belief, the mechanism of the cyber-attack was a known and foreseeable risk to Defendants, and Defendants were on notice that failing to take steps necessary to secure the IRAs from those risks left that property in a dangerous condition.

7. In addition, Defendants and their employees failed to properly monitor the computer network and systems that maintained the IRAs. Had Defendants properly monitored their property, they would have discovered the intrusion sooner.

8. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendants.

9. Accordingly, Plaintiff brings this action against Defendants seeking to redress their unlawful conduct.

PARTIES

10. Plaintiff Marshall Griffin is a resident and citizen of the city of Danville in the State of California. Plaintiff Griffin is acting on his own behalf and on behalf of others similarly situated. Mr. Griffin received notice of the Data Breach from Defendants on or about February 9, 2022.

11. Defendant IRA Financial is a South Dakota Trust company with its principal place of business at 5024 S. Bur Oak Place, Suite 200, Sioux Falls, SD 57108.

12. Defendant Gemini is a cryptocurrency exchange with its principal place of business at 600 Third Avenue, 2nd Floor, New York, NY 10016.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

14. This Court has personal jurisdiction over Defendants because a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

15. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District; and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

INTRADISTRICT ASSIGNEMTN

16. Pursuant to Civil Local Rule 3-2(c-d), a substantial part of the events giving rise to the claims herein arose in Contra Costa County, California and this action should be assigned to the San Francisco Division or the Oakland Division.

FACTUAL ALLEGATIONS

Background

17. IRA Financial is a South Dakota state chartered custodian under 408(a)(2) and a bank custodian defined under 408(n). It is regulated and licensed by the South Dakota Division of Banking.

18. IRA Financial enables consumers to open IRAs online and manage their retirement funds.

19. Founded in 2010, IRA Financial claims to have assisted over 28,000 clients in all 50 states invest more than $4.6 billion in alternative assets. IRA Financial has over 67 employees located in 5 states and claims to be the fastest growing provider of self-directed retirement accounts in the country.

20. On information and belief, IRA Financial has over $4.9 worth over retirement funds under the company's management.

21. IRS claims to be the "leader in Self-Directed Retirement Solutions." They promise to "establish, custody and administer your Self-Directed IRA."

22. IRA Financial claims consumers can "[d]o everything on our app," including "open your account, roll over your funds, and start investing all from the palm of your hand."

23. IRA Financial Trust's charter allows it to establish and administer self-directed IRA, Roth, SIMPLE Accounts, SEP Accounts, 401(k) plan accounts, Health Savings Accounts, and Coverdell Education Savings Accounts.

24. IRA Financial also claims it can simplify "how you invest your retirement funds in alternative assets" such as cryptocurrency.

25. According to Investopedia:

> A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

26. IRA proclaims "[w]hether the investment is made via the IRA custodian or our Checkbook Control IRA LLC, clients who want to invest in non-traditional assets like real estate,

precious metals, or cryptocurrencies will find that ***we offer secure*** and expert services at a fair price."

27. One of the cryptocurrencies users can invest in through IRA Financial is Bitcoin. Bitcoin is essentially the first (and most popular) cryptocurrency. A single Bitcoin presently trades for around $42,000 USD.

28. IRA Financial advertises to accountholders that they can seamlessly invest in Bitcoin (and other cryptocurrencies) thanks to their partnership with Gemini, a leading digital currency exchange and custodian.

29. According to IRA Financial, "[w] have integrated with Gemini Exchange, a leading digital currency exchange and custodian, to allow investors to purchase cryptocurrency investments directly through our digital retirement app. The new integration enables investors to buy and sell crypto without the need of an LLC (Limited Liability Company) or third-party broker-firm."[1]

30. IRA Financial further boasts:

> Now, investors can use their retirement funds to buy all the major cryptocurrencies directly through Gemini, one of the leading US cryptocurrencies exchange. Our new cryptocurrency solution is the first to allow retirement holders to hold cryptocurrencies in an IRA directly on an exchange. Clients can now control their transaction costs by avoiding the need for costly LLCs and Brokers, **but more importantly, trust Gemini as the licensed and qualified custodian of their cryptocurrency private key. It is our strong belief that the best and safest way to purchase Bitcoin and other cryptocurrency with IRA funds is with our digital solution**. IRA Financial clients can perform transactions any time and will gain complete control over their cryptos.

[1] https://www.irafinancialgroup.com/learn-more/self-directed-ira/bitcoin-investing-with-a-self-directed-ira/.

31. One of IRA Financial's focal points with respect to advertising to consumers is "Security" and "Trust".[2] IRA Financial boasts "Trust is our name."

32. IRA Financial represents to account holders they will have "total control" over their accounts.[3]

33. IRA Financial promises accountholders it has "Industry-leading technology" that allows it to provide cutting-edge "Infrastructure Security" and "Internal Controls."

34. In its Privacy Policy, IRA Financial further promises consumers: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[4]

35. Gemini likewise boasts to consumers about the safety of its platform:

> [T]he first trusted platform that focused on strong security controls and compliance. Today, every employee at Gemini continues our founders' focus on security and compliance, in order to build trust. Gemini has built a leading security program focused on developing innovative security solutions to help protect and secure our customers and their assets. We have also invested considerable resources to remain transparent about our security posture, through third party security assessments, including our SOC2 Type 2, ISO 27001, and annual penetration testing.[5]

36. Gemini claims it has "Industry Leading Security Controls". In fact, Gemini claims "Trust is our product, which begins by building and maintaining a secure customer experience."

37. Gemini represents to consumers it: "build[s] innovative security solutions to better protect our users and their accounts"; "has implemented leading security controls designed to mitigate the risk of insider threats"; "is passionate about building the most secure infrastructure

---

[2] https://www.irafinancialtrust.com/security/.
[3] https://www.irafinancialtrust.com/gemini-exchange-investing-in-cryptos-with-an-ira/.
[4] https://www.irafinancialtrust.com/privacy-policy/.
[5] https://www.gemini.com/security.

to protect and manage sensitive key material"; and "has embraced regulations and third party assessments that demonstrate our commitment to a safe and secure experience."

38. Gemini further boasts its "Trust and Safety Team has adopted…industry leading practices to help protect our users from fraud and abuse while using the Gemini platform."[6]

39. Gemini claims it "take[s] a number of measures to safeguard your account, like requiring multi-factor authentication and verification of new devices."

40. Gemini also represents to consumers it "rel[ies] on the same techniques used by leading financial institutions to review and approve new user accounts in order to limit fraud and abuse."

41. On information and belief, in the course of entering into account holder agreements with consumers, including Plaintiff and Class Members, Defendants promised to provide confidentiality and adequate security for customer data and the monies placed in their accounts through their applicable privacy policy and through other disclosures.

42. Based on the aforementioned promises and representations, Plaintiff, like all other Class Members, placed their trust in Defendants and allowed them to maintain and hold in trust the monies placed into his IRA.

The Data Breach

43. On February 8, 2022, Defendants discovered that certain IRA Financial customers had unauthorized withdrawals of cryptocurrency from their Gemini cryptocurrency wallets.

44. Defendants investigated the unauthorized activity and engaged third-party forensic specialists to conduct an investigation of the incident.

[6] https://www.gemini.com/trust-and-safety.

45. On February 24, 2022, the investigation determined that an unauthorized actor gained access to certain IRA Financial customer information, including their names, Social Security numbers, and financial account numbers.

46. In addition, it was determined that a number of IRA Financial customers had cryptocurrency stolen from their accounts.

47. In the wake of the Data Breach, IRA sent the following notification to impacted customers confirming the "affected assets have been identified as likely unrecoverable":

Good morning,

I would like to share an update on the February 8, 2022, incident that affected a limited subset of IRA Financial Trust customers. I have a personal relationship with many of you, one that's built on mutual trust. I want you to know how much I care about your individual situation and how seriously I take your concerns. IRA Financial Trust is committed to keeping our customers apprised of new developments.

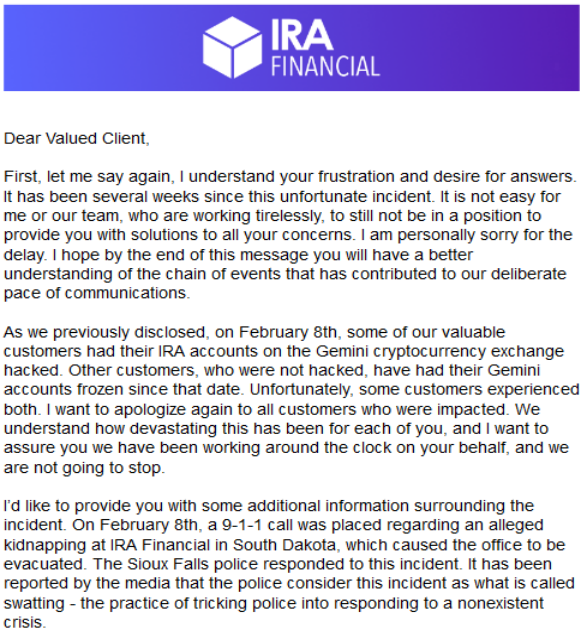
The preliminary findings of our investigation found that a small amount of affected assets were not transferred off the Gemini cryptocurrency exchange. We are in the process of restoring those assets back into their respective customer accounts. A small amount of affected assets that were withdrawn from the exchange have been identified as potentially recoverable. We are using all available resources to recover those assets. However, we cannot ensure the recoverability of these assets or put a timeline on those efforts.

At this time, unfortunately, the rest of the affected assets have been identified as likely unrecoverable. I am extremely disappointed about this development. But - we are actively exploring all potential avenues to address victims' losses. IRA Financial Trust has tendered a claim to IRA Financial Trust's insurers. But as of today, it has not yet been confirmed any related losses will be covered by IRA Financial Trust's insurance. I want to assure you again – we are devoting all our attention to address and resolve this matter as quickly as possible.

We will continue to provide meaningful updates as they become available. This is a difficult situation that we understand is outside your control. And as I said earlier, I am doing all I can personally to dedicate all available resources toward this effort.

Thank you for your time and for being valued customers of IRA Financial Trust.

48. Then, on or about March 3, 2022, IRA Financial sent another notification to its customers acknowledging they had been hacked:



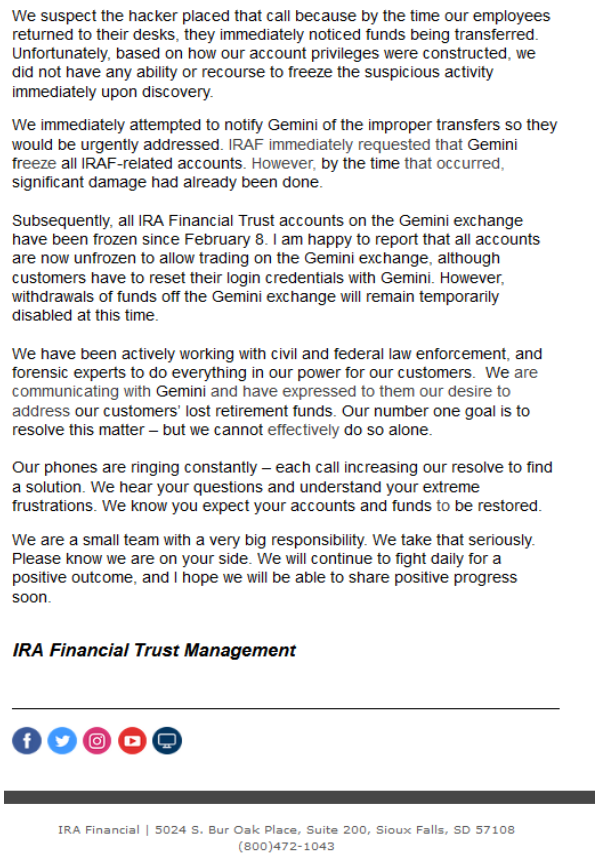
IRA FINANCIAL

Dear Valued Client,

First, let me say again, I understand your frustration and desire for answers. It has been several weeks since this unfortunate incident. It is not easy for me or our team, who are working tirelessly, to still not be in a position to provide you with solutions to all your concerns. I am personally sorry for the delay. I hope by the end of this message you will have a better understanding of the chain of events that has contributed to our deliberate pace of communications.

As we previously disclosed, on February 8th, some of our valuable customers had their IRA accounts on the Gemini cryptocurrency exchange hacked. Other customers, who were not hacked, have had their Gemini accounts frozen since that date. Unfortunately, some customers experienced both. I want to apologize again to all customers who were impacted. We understand how devastating this has been for each of you, and I want to assure you we have been working around the clock on your behalf, and we are not going to stop.

I'd like to provide you with some additional information surrounding the incident. On February 8th, a 9-1-1 call was placed regarding an alleged kidnapping at IRA Financial in South Dakota, which caused the office to be evacuated. The Sioux Falls police responded to this incident. It has been reported by the media that the police consider this incident as what is called swatting - the practice of tricking police into responding to a nonexistent crisis.



We suspect the hacker placed that call because by the time our employees returned to their desks, they immediately noticed funds being transferred. Unfortunately, based on how our account privileges were constructed, we did not have any ability or recourse to freeze the suspicious activity immediately upon discovery.

We immediately attempted to notify Gemini of the improper transfers so they would be urgently addressed. IRAF immediately requested that Gemini freeze all IRAF-related accounts. However, by the time that occurred, significant damage had already been done.

Subsequently, all IRA Financial Trust accounts on the Gemini exchange have been frozen since February 8. I am happy to report that all accounts are now unfrozen to allow trading on the Gemini exchange, although customers have to reset their login credentials with Gemini. However, withdrawals of funds off the Gemini exchange will remain temporarily disabled at this time.

We have been actively working with civil and federal law enforcement, and forensic experts to do everything in our power for our customers. We are communicating with Gemini and have expressed to them our desire to address our customers' lost retirement funds. Our number one goal is to resolve this matter – but we cannot effectively do so alone.

Our phones are ringing constantly – each call increasing our resolve to find a solution. We hear your questions and understand your extreme frustrations. We know you expect your accounts and funds to be restored.

We are a small team with a very big responsibility. We take that seriously. Please know we are on your side. We will continue to fight daily for a positive outcome, and I hope we will be able to share positive progress soon.

IRA Financial Trust Management

IRA Financial | 5024 S. Bur Oak Place, Suite 200, Sioux Falls, SD 57108
(800)472-1043

49. In the wake of the Data Breach, Bloomberg reported that "Hackers Snagged $36 million in Crypto in Breach of IRA Financial."[7]

50. Immediately following the Breach, Gemini and IRA Financial started pointing the finger at one another as to who was to blame. According to a Bloomberg report, "IRA Financial spokesperson Maria Stagliano said **the company's investigation is primarily focused on security controls that IRA Financial claims weren't offered or available from Gemini**. She declined to say which controls IRA Financial had in place."

51. However, Gemini lays the blame at the feet of IRA Financial. According to an article from CoinDesk:

[7] https://www.bloomberg.com/news/articles/2022-02-14/ira-financial-hacked-36-million-in-cryptocurrency-stolen.

> Although our investigation remains ongoing, the facts discovered to date indicate that transfer requests were made by utilizing properly authenticated accounts controlled by IRA Financial Group, which were used to execute asset transfers to another account," the firm wrote late Sunday night. "At the time, these requests complied with IRA's approval processes and appeared to Gemini to be legitimate, authorized transactions. To date, our investigation has found no indication of any unauthorized access to your account resulting from any security failure or breach of Gemini systems. **This finding would place the blame entirely on IRA Financial**. It would also, in Gemini's telling, absolve it of any responsibility to cover the loss with its own insurance policy. Gemini advised the customer to ask IRA Financial about its insurance policy.[8]

52. On information and belief, neither of the Defendants had adequate data security measures in place to prevent the stunning Breach despite their representations and promises to accountholders that security is their top priority.

53. Defendants have not compensated the victims of their negligence nor have they offered any identity theft monitoring services or assistance.

Defendants Were Aware of the Data Breach Risks

54. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their customers' private information confidential and accounts protected from unauthorized access and disclosure.

55. Plaintiff and Class Members entrusted Defendants with their private information and monies with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to employ reasonable care to keep such property confidential and secure from unauthorized access.

[8] https://www.coindesk.com/business/2022/02/14/drained-crypto-accounts-at-ira-financial-leave-victims-searching-for-answers/.

56. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the Data Breach.

57. It has been well-reported that the banking/credit/financial services industry is one of the most "at-risk" industries when it comes to cybersecurity attacks.[9] Attacks against the financial sector increased 238% globally from the beginning of February 2020 to the end of April, with some 80% of financial institutions reporting an increase in cyberattacks, according to cyber security firm VMware.

58. For example, in 2019, Capital One experienced a data breach that resulted in the personal data of more than 100 million customers being stolen.[10]

59. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

60. Defendants themselves were aware the risks of cyberattacks as evidenced by the fact that they advertise to customers how secure their platforms supposedly are to transact on.

61. In fact, according to reports, Defendants knew "something was amiss" even before the Data Breach occurred, and yet they still failed to take appropriate action. As CoinDesk reports:

> [A] memo distributed to customers on the morning of the breach hints that even hours before the hack, IRA Financial knew something was amiss.

---

[9] *See, e.g., https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/financial-services-risk-cyber.html.*

[10] https://www.nytimes.com/2021/12/23/business/capital-one-hacking-settlement.html#:~:text=The%20breach%20involved%20the%20personal%20data%20of%20more%20than%20100%20million%20customers.&text=Capital%20One%20has%20agreed%20to,100%20million%20people%20in%202019.

> "We have reason to believe that there are some bad actors posing as IRA Financial employees looking for crypto account-related information," the email read. It warned users to remain wary of phishers.[11]

62. The CoinDesk report indicates that Defendants may have fallen victim to one of the oldest cyberattacks in the book – a phishing scheme, which typically involves an employee clicking on an unknown malicious link.

63. Simply put, with the increase in cyberattacks in Defendant's industry, and the attendant red flags, the Data Breach was completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

64. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[12] Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[13]

65. Defendants knew, or reasonably should have known, of the importance of safeguarding the private information and monies of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result of a breach.

---

[11] https://www.coindesk.com/business/2022/02/14/drained-crypto-accounts-at-ira-financial-leave-victims-searching-for-answers/.

[12] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Nov. 29, 2021).

[13] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of retirement monies which they may never have an opportunity to recover since many are no longer in the workforce. They are incurring and will continue to incur such damages well into the future.

67. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the private information and monies of Plaintiff and Class Members.

Defendants Failed to Comply with FTC Guidelines

68. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

69. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' private information and monies constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

73. To prevent and detect cyberattacks, including the attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

f. Set anti-virus and anti-malware programs to conduct regular scans automatically;

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

74. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

1. **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

2. **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

3. **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

4. **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.

5. **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

6. **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

7. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[14]

75. Defendants were at all times fully aware of their obligation to protect the private information and monies of their customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

[14] https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 29, 2021).

76. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

77. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

78. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach.

Defendants' Breach

79. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their

computer systems, networks, and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' private information and monies;

c. Failing to properly monitor their data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

80. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' private information and monies.

81. Accordingly, Plaintiff and Class Members have been damaged by the loss of their private information and monies pilfered from their accounts.

82. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

In Addition to the Money Stolen From Their Accounts, the Data Breach Has Caused Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

83. Defendants were well aware that the private information it collected is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

84. 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."[15]

85. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

86. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim.

87. For example, armed with just a name and date of birth, a data thief can use 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.

88. Social engineering is a form of hacking whereby a data thief uses previously

---

[15] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 29, 2021) ("GAO Report").

acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

89. The FTC recommends that identity theft victims take several steps 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 seven years if someone steals their 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.[16]

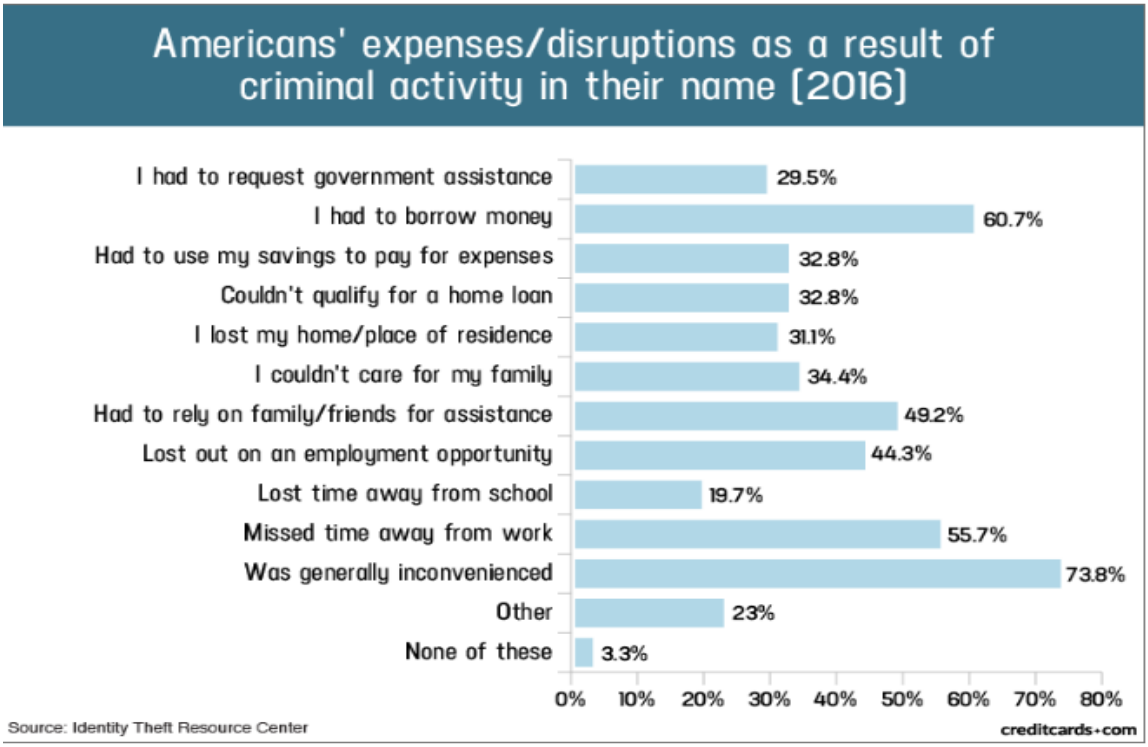
90. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

91. 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.

92. 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.

[16] *See* https://www.identitytheft.gov/Steps (last accessed Sept 22, 2021).

93. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[17]



94. What's more, theft of private information is also gravely serious. PII is a valuable property right.[18]

95. 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 Private Information has considerable market value.

---

[17] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Nov. 29, 2021).

[18] *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).

96. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when private information and/or financial information is stolen and when it is used.

97. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in 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 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.

See GAO Report, at 29.

98. Private information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

99. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a substantial and immediate present risk of fraud and identity theft that will continue for many years.

100. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

101. Sensitive private information such as Social Security numbers can sell for as much as $363 according to the Infosec Institute.

102. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of 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.

103. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

104. Each of these fraudulent activities is difficult to detect. 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.

105. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

106. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he 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."[19]

107. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit

---

[19] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Nov. 29, 2021).

card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[20]

108. At all relevant times, Defendants knew or reasonably should have known these risks, the importance of safeguarding their customers' private information and monies, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

109. Defendants entirely fail to provide any compensation for the private information and monies stolen in the Data Breach.

110. Plaintiff and Class Members have not received any compensation for the money stolen from their IRAs.

111. Moreover, Plaintiff and Class Members have been damaged by the compromise of their private information, including their Social Security numbers and financial account information, in the Data Breach.

112. Plaintiff and Class Members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

113. Plaintiff and Class Members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegality

---

[20] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at: http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 29, 2021).

based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

114. Plaintiff 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.

115. Plaintiff and Class members also suffered a loss of value of their private information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

116. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

117. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. 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

118. Moreover, Plaintiff and Class Members have an interest in ensuring that their private information, which is believed to remain in the possession of Defendants, 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 personal and financial information is not accessible online and that access to such data is password protected.

119. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their private information —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.

120. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Griffin's Experience

121. Plaintiff Griffin became an accountholder with IRA Financial in or around April 2021.

122. Plaintiff Griffin became an accountholder with Gemini in or around May 2021.

123. Plaintiff Griffin reviewed and relied on the representations alleged herein when he decided to open accounts with Defendants and place his monies in trust with Defendants.

124. Plaintiff Griffin purchased cryptocurrency with his accounts and through Defendants, in part, based on these representations and promises.

125. Plaintiff Griffin never would have opened accounts with Defendants if he knew they did not have adequate security measures in place.

126. In making these transactions and others with Defendants, Plaintiff Griffin entrusted private information and monies to Defendants with the reasonable expectation and understanding that Defendants would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that valuable property from unauthorized users or disclosure.

127. On February 8, 2022, there were two unauthorized transactions from Plaintiff Griffin's account whereby a total of 2 Bitcoins (worth approximately $85,000) were transferred out his account to cybercriminals as a result of the Data Breach.

128. Plaintiff Griffin has not been compensated for the monies stolen from his account.

129. Moreover, Plaintiff Griffin has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the

telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

130. Plaintiff Griffin stores all documents containing his sensitive information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the few online accounts that he has.

131. In addition to the stolen monies, Plaintiff Griffin has suffered actual injury in the form of damages to, and diminution in, the value of his private information– a form of intangible property that Plaintiff Griffin entrusted to Defendants. This private information was compromised in, and has been diminished as a result of, the Data Breach.

132. Plaintiff Griffin has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

133. Plaintiff Griffin has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his private information resulting from the Data Breach.

134. Plaintiff Griffin has a continuing interest in ensuring that his private information and monies that, upon information and belief, remain in the possession of Defendants, is protected and safeguarded from future data breaches.

135. As a result of the Data Breach, Plaintiff Griffin is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS ALLEGATIONS

136. Plaintiff brings this nationwide class action pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), individually and on behalf of all members of the Class:

> All natural persons residing in the United States whose private information or monies was compromised in the Data Breach initially discovered by Defendants on or about February 8, 2022 (the "Class").

137. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

138. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

139. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes hundreds of thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class Members is in the possession and control of Defendants and will be ascertainable through discovery.

140. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including, without limitation:

a. Whether Defendants unlawfully maintained, lost or disclosed Plaintiff's and Class Members' private information and/or monies;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their private information and/or monies;

f. Whether Defendants breached duties to Class Members to safeguard their private information and/or monies;

g. Whether cyber criminals obtained Class Members' private information and/or monies in the Data Breach;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' conduct violated federal law;

l. Whether Defendants' conduct violated state law; and

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

141. Typicality. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had his private information and IRA compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of Defendants, described throughout this Complaint, and assert the same claims for relief.

142. Adequacy. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

143. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would

therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendants' wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

144. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading their data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

145. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

146. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their private information and/or monies;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their private information and/or monies;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiff and Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

FIRST CLAIM
Negligence
(On Behalf of Plaintiff and the Class)

147. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 145.

148. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their private information and/or monies placed in their IRA from unauthorized third parties.

149. The legal duties owed by Defendants to Plaintiff and Class Members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting the private information and/or monies of Plaintiff and Class Members in Defendants' possession;

b. To protect the private information and/or monies of Plaintiff and Class Members in Defendants' possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

150. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

151. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiff and Class Members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect their private information and/or monies and by not complying with industry standards.

152. Defendants breached their duties to Plaintiff and Class Members. Defendants knew or should have known the risks of collecting, storing and maintaining the private information and/or monies and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

153. Defendants knew or should have known that their security practices did not adequately safeguard the private information and/or monies of Plaintiff and Class Members.

154. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the private information

and/or monies of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the private information and/or monies of Plaintiff and Class Members during the period it was within Defendants' possession and control.

155. Defendants breached the duties they owe to Plaintiff and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' private information and/or monies and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach; and

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack.

156. Due to Defendants' conduct, Plaintiff and Class Members are entitled to actual damages and credit monitoring. Credit monitoring is reasonable here. The private information taken can be used for identity theft and other types of financial fraud against them immediately and for years to come.

157. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219.00 to $358.00 per year.

158. As a result of Defendants' negligence, Plaintiff and Class Members suffered injuries that may include:

(i) Stolen monies from their IRA;

(ii) actual identity theft;

(iii) the lost or diminished value of their private information;

(iv) the compromise, publication, and/or theft of private information;

(v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their private information;

(vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

(vii) the continued risk to their private information, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the private information in their continued possession;

(viii) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

159. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

SECOND CLAIM
Negligence Per Se
(On Behalf of Plaintiff and the Class)

160. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 158.

161. 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 businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

162. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect the private information and/or monies in their possession and not complying

with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of private information and/or monies in their possession, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the property at issue in this case—including monies placed in IRAs which amounted to $36 million stolen and other personal information such as Social Security numbers.

163. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

164. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

165. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

166. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

i. Stolen monies from their IRA;

ii. actual identity theft;

iii. the lost or diminished value of private information;

iv. the compromise, publication, and/or theft of private information;

v. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their private information;

vi. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

vii. the continued risk to their private information, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the private information in their continued possession;

viii. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

167. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their private information and/or monies, which remains in Defendants' possession and is subject to further unauthorized access and disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the property in their continued possession.

THIRD CLAIM
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

168. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 166.

169. When Plaintiff and Class Members provided their private information and monies to Defendants in exchange for Defendants' products and services, they entered into implied contracts with Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their private information and monies.

170. Defendants solicited and invited Plaintiff and Class Members to provide their private information and monies as part of Defendants' regular business practices and as essential to the sales and transactions entered into between Defendants on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendants on the other hand. Plaintiff and Class Members

accepted Defendants' offers by providing their private information and monies to Defendants in connection with their purchases from Defendants.

171. Defendants benefitted from these transactions in a number of ways, including, among other things, charging fees associated with the transactions made on their respective platforms.

172. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

173. Plaintiff and Class Members paid money to Defendants to purchase products or services from them. Plaintiff and Class Members reasonably believed and expected that Defendants would use part of the funds received as a result of the purchases or services provided to obtain adequate data security. Defendants failed to do so.

174. Plaintiff and Class Members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from the continued use of Defendants' services—that Defendants would adequately safeguard their private information and moneys. Defendants failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

175. Plaintiff and Class Members value data security and would not have provided their private information and moneys to Defendants in the absence of Defendants' implied promise to keep the property reasonably secure.

176. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

177. Defendants breached their implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

178. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, request judgment against Defendants and that the Court grant the following:

1. An order certifying the Class as defined herein, and appointing Plaintiff and her counsel to represent the Class;

2. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and Class Members;

3. An order requiring Defendants to:

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

   b. Engage third-party security auditors and internal personnel to run automated security monitoring;

   c. Audit, test, and train their security personnel regarding any new or modified procedures;

   d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

   e. Conduct regular database scanning and security checks;

   f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

   g. Purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Meaningfully educate Plaintiff and Class Members about the threats they face as a result of the loss of their private information to third parties, as well as the steps they must take to protect themselves.

4. An award of compensatory, statutory, and nominal damages in an amount to be determined at trial;

5. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class Members;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands this matter be tried before a jury.

Dated: March 18, 2021

Respectfully Submitted,

/s/ Alex R. Straus

Alex R. Straus (SBN 321366)
astraus@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
T: 917-471-1894
F: 865-522-004

Gary M. Klinger, Esq.*
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
T: (847) 208-4585

Attorneys for Plaintiff and Putative Class

* Pro Hac Vice Application Forthcoming