UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

PAUL BERGER, *individually, and on behalf of all others similarly situated*, Plaintiff, v. MERCER ADVISORS, INC. and MERCER GLOBAL ADVISORS, INC. Defendants.	**Case No. _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff PAUL BERGER ("Plaintiff"), by and through his undersigned counsel, on behalf of himself and a class of all other similarly situated persons, files this Class Action Complaint against Mercer Advisors, Inc. and Mercer Global Advisors, Inc., (together, "Mercer"). Plaintiff's allegations are made based upon personal knowledge, his own acts, and upon information and belief and investigation of counsel, as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this action against Mercer for its failure to properly secure and safeguard highly valuable, protected, personally identifiable information and for its failure to comply with industry standards to protect information systems that contain and/or are utilized to transfer the personal information of Plaintiff and Class members. Plaintiff has been, and continues to be, harmed as a result of Mercer's failure to properly secure and safeguard its customers highly valuable, protected, personally identifiable information including, *inter alia*, names, contact information, full or partial Social Security numbers, emergency contact details, contract

documents, legal documents, and other personally identifiable information (collectively, "PII" or "Personal Information"); and for its failure to comply with industry standards to protect information systems that contain PII.

2. Mercer is a national wealth management and investment advisory firm that collects, stores, and maintains highly sensitive personal and financial information from its clients as part of providing ongoing financial planning and advisory services.

3. On or about February 16, 2026, an extortion-oriented cybercrime group known as ShinyHunters claimed responsibility for an unauthorized intrusion into systems associated with Mercer, asserting that it had accessed and exfiltrated over 5 million records belonging to the firms' clients and internal operations.[1]

4. The group issued a 48-hour ultimatum to Mercer, threatening to leak the records it had stolen if Mercer refused to pay a ransom; warning Mercer to "[m]ake the right decision, don't be the next headline."[2] When its demands were not met, ShinyHunters published the records to the dark web.

5. According to independent reporting that analyzed the leaked datasets, the alleged breach involved approximately 5.7 million individual records containing names, contact information, full or partial Social Security numbers, emergency contact details, contract

[1] Cybernews, Barron's top investment advisors threatened with 48-hour ultimatum "don't be the next headline" (Feb. 17, 2026) https://cybernews.com/security/shinyhunters-mercer-beacon-ria-breach/ (last visited Feb, 25, 2026).

[2] *Id*.

documents, legal documents, and other personally identifiable information that was routinely collected and maintained by Mercer.[3]

6. In its ultimatum, ShinyHunters characterized the exfiltrated information as highly sensitive and implied that disclosure of that information would imminently expose individual clients and internal corporate documents to unauthorized third parties, thereby substantially increasing the risk that any person whose information was included in the dataset would suffer identity theft, fraud, or other misuse of their personal and financial information.

7. As a direct result of the unauthorized access and disclosure of Plaintiffs' and Class members' personal and financial information, those individuals are put at heightened risk of identity theft, financial fraud, phishing, and other harms, thereby causing substantial and ongoing damages..

8. Plaintiff brings claims for negligence, negligence *per se*, unjust enrichment, and breach of implied contract, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in Mercer's possession in order to prevent incidents like the Data Breach from reoccurring in the future.

II. PARTIES

9. Plaintiff Paul Berger, at all relevant times, is a citizen and resident of the District of Columbia.

[3] Cybernews, ShinyHunters reveals +5M records after Wall Street ignores "final warning" (Feb. 23, 2026) https://cybernews.com/security/shinyhunters-mercer-beacon-data-breach/ (last visited Feb, 25, 2026).

10. Defendant Mercer Advisors, Inc. is a corporation organized and existing under the laws of Delaware that maintains a principal place of business at 1200 17th Street, Suite 2000, Denver, Colorado.

11. Defendant Mercer Global Advisors, Inc. is a wholly owned subsidiary of Mercer Advisors, Inc. It is also a corporation organized and existing under the laws of Delaware that maintains a principal place of business at 1200 17th Street, Suite 2000, Denver, Colorado.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Mercer.

13. This Court has personal jurisdiction over Mercer because Mercer maintains its principal place of business in this District, and a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

14. Venue is proper under 28 U.S.C. § 1391(a)(2), (b)(1)-(3), and (c)(2) because Mercer's principal place of business is located in this District, Mercer conducts substantial business in this District, and a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. Mercer's Business

15. Mercer is a national wealth management and financial planning firm specializing in financial planning, investment management, tax planning and preparation, estate planning, insurance solutions, trustee services, retirement planning, family office services, private markets investing, wealth management.[4]

16. In the ordinary course of its business, Mercer collects and maintains the PII of its current and former customers, including but not limited to:

Contact Information	• Full legal name • Email address • Mailing address and physical address (if different) • Preferred phone number, Identification Data
Identification Data	• Social Security Number or Tax Identification Number • State or local identification card number • Date of birth
Profile Information	• Login credentials to establish access to our client portal • Investment risk tolerance, preferences, and objectives • Biographical details (e.g., education, employer), Interests (e.g., boating, skiing, traveling) • Login credentials to review other accounts, if permitted by client • Family member data provided by client (e.g., family members' name, gender, age, and date of birth) • Estate plan documents
Financial Data	• Income

[4] InvestmentNews, Mercer Advisors, https://www.investmentnews.com/companies/mercer-advisors/265050?utm (last visited Feb. 25, 2026).

	• Economic status (e.g., high-net-worth) • Tax status • Tax returns • Financial account details provided by client • Investment holdings • Account balances and contributions • Asset levels and ability to invest
Marketing Data	• Preferences regarding communication about our services, events, and publications
Payment Data	• Credit card information • Billing information.[5]

17. Mercer made promises and representations to Plaintiff and Class Members that the PII it solicited and collected from them would be kept safe and confidential, assuring Plaintiff and Class Members that "Mercer Advisors employs technical, organizational, and physical safeguards designed to protect the personal information we collect."[6]

18. By virtue of its role as a financial-services firm and in light of these representations, Mercer owed Plaintiff and Class Members a duty to exercise reasonable care in collecting, storing, and using their PII, and to maintain appropriate data security safeguards consistent with industry standards, regulatory guidance, and common-law obligations. Plaintiff and Class Members had a reasonable expectation that Mercer would comply with its obligations related to their PII.

19. Mercer failed to comply with its obligations, resulting in the Data Breach.

[5] *Mercer Privacy Policy Effective as of February 10, 2023*, Mercer, https://www.merceradvisors.com/privacy-policy/ (last visited Feb, 25, 2026).

[6] *Id*.

B. Mercer Obtains, Collects, Stores, Uses, and Derives a Benefit from the PII of Plaintiff and Class Members.

20. Defendant acquires, collects, and stores a significant amount of PII belonging to Plaintiff and Class Members. Defendant uses this PII to provide goods and services, making a profit therefrom. Defendant would not be able to obtain revenue if not for the acceptance and use of this PII.

21. As a condition of utilizing or purchasing Mercer's products and services and/or their employment with Mercer, Plaintiff and Class Members were required to entrust their highly sensitive PII to Mercer.

22. By collecting and obtaining Plaintiff's and the Class Members' PII, either directly or indirectly, Defendant assumed legal and equitable duties to Plaintiff and the Class Members to protect and safeguard their PII from unauthorized access and intrusion.

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted their PII to Defendant absent a commitment to safeguard that information.

24. Defendant recognizes this duty in their respective Privacy Policies and marketing to its customers and employees.

25. Defendant's assurances of maintaining high standards of cybersecurity demonstrates it recognizes it has a duty to use reasonable measures to protect the PII it collects and maintains.

26. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use their PII for business purposes only, and to make only authorized

disclosures of their PII. The Data Breach occurred because Defendant failed to honor its commitments.

27. Defendant violated its explicit privacy statements and failed to adopt reasonable and appropriate security practices and procedures, including administrative, physical security, and technical controls, to safeguard Plaintiff's and Class Members' PII.

28. As a result, Plaintiff's and Class Members' PII was accessed and stolen from Defendant's inadequately secured data systems in massive and preventable Data Breach

C. The Data Breach

29. On or about February 16, 2025, Mercer was the victim of a cyber extortion attack by a notorious group of hackers using the online moniker "ShinyHunters." The Data Breach compromised 5.7 million individual records including records containing Plaintiff's and Class Members' sensitive PII.[7]

30. ShinyHunters has been linked to several of the largest data breaches in history, and the group's "pay or leak" reputation involves demanding multimillion-dollar ransoms in cryptocurrency, with the threat of public data dumps on their dedicated leak site if negotiations fail.

31. The group's extortion tactics often escalate quickly and with real-world consequences, such as swatting attacks and the dissemination of threats of physical violence to

[7] Cybernews, ShinyHunters reveals +5M records after Wall Street ignores "final warning" (Feb. 23, 2026) https://cybernews.com/security/shinyhunters-mercer-beacon-data-breach/ (last visited Feb, 25, 2026).

coerce payment. In a notable escalation of these "terror" tactics, ShinyHunters has been observed publishing lists of federal employees accompanied by explicit threats of murder.[8]

32. After obtaining the records, the attackers attempted to extort Mercer to pay a ransom by threatening to disclose the information.

33. When Mercer refused to comply with the ransom demand, ShinyHunters released the documents publicly on the dark web on or about February 18, 2026.

34. Class Members now face the threat of years of potential phishing and extortion attempts. For example, by linking the stolen email addresses with identifiable profile details such as a user's follower count or avatar, cybercriminals can create highly convincing phishing emails, including messages that impersonate Mercer support and reference specific account information to gain trust.

35. These and other threats resulting from the Data Breach will now require Plaintiffs to engage in ongoing and constant monitoring of their financial and personal records.

D. The Value of Private Information and Effects of Unauthorized Disclosure

36. Mercer was well aware that the protected PII which they acquire is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

37. Mercer also knew that a breach of their computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

[8] Unit2218, Harassment, Scare Tactics, & Why Victims Should Never Pay ShinyHunters (Feb. 2. 2026), https://blog.unit221b.com/dont-read-this-blog/harassment-scare-tactics-why-victims-should-never-pay-shinyhunters (last visited Feb. 25, 2026)

38. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] 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."[10]

39. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

40. Numerous sources cite dark web pricing for stolen identity credentials.[11] For example, Private Information can be sold at a price ranging from $40 to $200.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

41. Identity thieves use stolen Private Information for a variety of crimes, including credit card fraud, phone or utilities fraud, extortion, and bank/finance fraud.

---

[9] 17 C.F.R. § 248.201 (2013).

[10] *Id.*

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 25, 2026).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 25, 2026).

[13] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 25, 2026).

42. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

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

44. Moreover, the fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (" GAO"), which conducted a study regarding data breaches:[14]

> [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.

45. When combined with other publicly available data, any PII element can be used to build full identity profiles, known as "Fullz" packages, which are frequently exploited in financial fraud schemes. "Fullz" is fraudster-speak for data that includes a victim's information, including name, address, SSN, date of birth, and more.

46. With Fullz packages, cybercriminals can cross-reference two (or more) sources of PII to marry unregulated data available elsewhere (e.g., address or phone number) to criminally stolen data to assemble shockingly accurate and complete dossiers on individuals.

---

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 25, 2026).

47. Compromised PII, whether alone or as part of a Fullz package, is highly valuable to cybercriminals, who can use it to engage in a wide range of fraudulent activities, including committing unemployment insurance fraud, opening unauthorized financial accounts, and applying for government benefits.

48. This type of identity theft renders any compromised data—including seemingly innocuous PII, such as name and contact information—valuable. In the wrong hands, up-to-date names, addresses, phone numbers, and email addresses can be used to update, validate, and verify Fullz packages, which can then be used for nefarious purposes.

49. For example, a criminal actor can use an up-to-date Fullz package to bypass identity verification tools—which are often used in financial transactions (like loan applications), background checks, etc.—without detection. In a typical identity verification system, a user submits their PII, like their name, addresses, or date of birth. That customer-submitted PII is then cross-checked against "a trusted data set," including those from "credit bureaus, official government documents or mobile operator databases."

50. Thus, with an up-to-date Fullz package—which might include seemingly harmless information, like the identity theft victim's name and current address—a cybercriminal has the victim's up-to-date PII, which will match the victim's information from trusted data sources, like the credit bureaus. With this information, the criminal can then successfully pass identity verification systems without raising any red flags. In this way, Fullz packages, which are made possible by up-to-date and compromised elements of PII, enable fraudsters to carry out various forms of identity theft, including taking out fraudulent loans.

51. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

E. Mercer Failed to Comply with FTC Guidelines and Industry Best Practices

52. The Federal Trade Commission ("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 a factor in all business decision-making.

53. 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 network's vulnerabilities; and implement policies to correct any security problems.[15] 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.[16]

54. The FTC further recommends that companies not maintain PII longer than necessary 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

[15] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Feb. 25, 2026).

[16] *Id.*

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

55. The FTC also directs businesses to provide immediate notification to individuals impacted by a data breach is critical so that those impacted can take measures to protect themselves.

56. Here, Mercer has acted inexcusably by failing to provide timely notice to the individuals whose personal information was compromised in the Data Breach, despite its knowledge of the incident and its obligations to safeguard such information.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Mercer failed to properly implement the kind of basic data security practices that have led to successful FTC enforcement actions for violating Section 5 of the FTCA.

59. Mercer's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Mercer was at all times fully aware of their obligation to protect the Private Information of consumers. Mercer was also aware of the significant repercussions that would result from their failure to do so.

F. Mercer Failed to Comply with Industry Standards

61. As shown above, Mercer owed a duty of care to Plaintiff and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected their PII.

62. Several best practices have been identified that at a minimum should be implemented by financial service providers like Mercer, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the financial 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.

25. Despite the sensitivity of the PII and the heightened risk profile of wealth-management clients, Mercer's data-security measures were insufficient to prevent or promptly detect the ShinyHunters attack. Mercer failed to adopt, implement, and maintain reasonable security practices, including but not limited to:

- Adequate network segmentation;
- Robust access controls and least-privilege permissions;
- Timely patching and remediation of known vulnerabilities;
- Multi-factor authentication and credential-protection measures;

- Encryption of PII at rest and in transit;
- Effective intrusion-detection and logging; and
- Regular security audits and risk assessments.

G. Data Breaches are Preventable

64. Despite the growing body of publicly available information regarding the rise of ransomware attacks, vishing schemes, and other forms of cyberattacks that compromise PII, Defendant's approach to maintaining the privacy of Plaintiff's and Class Members' PII was inadequate, unreasonable, negligent, and reckless. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information Defendant was maintaining for Plaintiff and Class Members such as encrypting the information or deleting it when no longer needed, limiting employee access keys to PII, and adequately training its employees concerning cyber and ransomware attacks, which caused the exposure of Plaintiff's and Class Members' PII.

65. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[17]

66. Defendant could have prevented this Data Breach. It could have and should have implemented measures—as recommended by the U.S. Government—to prevent and detect cyberattacks and/or ransomware attacks, including, but not limited to, the following:

- **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.
- **Enable strong spam filters** to prevent phishing emails from reaching the end users and authenticate inbound email using

[17] Ransomware Prevention and Response, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Mar. 2, 2026).

technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- **Configure firewalls** to block access to known malicious IP addresses.
- **Patch operating systems, software, and firmware on devices**. Consider using a centralized patch management system.
- **Set anti-virus and anti-malware programs to conduct regular scans automatically**. Ensure these programs run automatic scans to detect and remove potential threats.
- **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.
- **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.
- **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.
- **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.
- **Disable Remote Desktop protocol (RDP)** if it is not being used.
- **Use application whitelisting**, which only allows systems to execute programs known and permitted by security policy.
- **Execute operating system environments or specific programs in a virtualized environment**. Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value** and implement physical and logical separation of networks and data for different organizational units.[18]

67. To prevent and detect cyberattacks and ransomware attacks, Defendant could and should have implemented the following preventive measures, as recommended by Microsoft's Threat Protection Intelligence Team:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
  - Remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise
- **Include IT Pros in security discussions**
  - Ensure collaboration among security operations, security admins, and information technology admins to configure servers and other endpoints securely
- **Build credential hygiene**
  - Use multifactor authentication or network level authentication and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications.[19]
  -

[18] *Id.*

[19] *See* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 2, 2026).

68. Similarly, Defendant could and should have implemented measures—also recommended by the U.S. Government—to prevent and detect cyberattacks and/or ransomware attacks, including the following recommendations:

- Know what personal information you have in your files and on your computers.
- Keep only what you need for your business.
- Protect the information that you keep.
- Properly dispose of information you no longer need. Create a plan to respond to security incidents.[20]

69. Finally, Defendant could and should have implemented the following measures—also recommended by the U.S. Government—to prevent and detect cyberattacks and/or ransomware attacks, including the following recommendations:

- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface.
- **Regularly patch and update software and operating systems to the latest available versions**. Prioritize timely patching of internet-facing servers that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….
- **Limit the use of RDP and other remote desktop services**. If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.
- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured and security features are enabled**. For example, disable ports and protocols not being used for business purposes.[21]

---

[20] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Mar. 2, 2026).

[21] *See* https://www.cisa.gov/resources-tools/resources/stopransomware-guide (last visited Mar. 2, 2026).

70. Because Defendant was collecting, storing, and transferring highly sensitive PII belonging to Plaintiff and Class Members, it could—and should—have implemented all of the above measures to prevent and detect cyberattacks.

71. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks or vishing attacks, resulting in the Data Breach and data thieves accessing and acquiring the PII of Plaintiff and millions of Class Members.

H. Data Breaches are Foreseeable and ShinyHunters is a Notorious Hacking Group that Employs Commonly Known Techniques

72. ShinyHunters is a notorious cybercriminal group that became widely known in 2020, gaining attention with high-profile data breaches.[22][23]

73. ShinyHunters was first widely known for selling 91 million user records from the Indonesian e-commerce platform Tokopedia on the dark web.[24] According to Forbes, "[i]n just the first two weeks of May 2020, a hacker, known only as ShinyHunters, offered an astonishing 200 million stolen data records for sale on the dark web. Not repurposed data from old breaches,

[22] Lily Hay Newman, ShinyHunters Is a Hacking Group on a Data Breach Spree, WIRED (May 21, 2020), available at https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/ (last visited Mar. 2, 2026).

[23] ShinyHunters, One of the Most Recognized Threat Actors Among the Hacking Community, WhiteBlueOcean (Feb. 16, 2021), available at https://www.whiteblueocean.com/newsroom/shinyhunters-one-of-the-most-recognised-threat-actors-among-the-hacking-community/ (last visited Mar. 2, 2026).

[24] BugCrowd, Glossary, ShinyHunters, https://www.bugcrowd.com/glossary/shinyhunters/ (last visited Mar. 2, 2026).

but fresh to the market and, therefore, very valuable. The surprising thing is that, until then, nobody had even heard of ShinyHunters."[25]

74. In 2020 alone, ShinyHunters was selling the following data batches on the dark web:[26]

- Vakina.com.br — 4.8 million records
- Truefire.com — 600,000 records
- Havenly.com — 1.3 million records
- Drizly.com — 2.4 million records
- Proctoru.com — 444,000 records
- Scentbird.com — 5.8 million records
- Appen.com — 5.8 million
- Homechef.com — 8 million records
- Chatbooks.com — 15 million records

75. Since then, ShinyHunters has gained even more notoriety for targeting companies across various sectors, including technology, education, media, and e-commerce, accumulating a significant track record of damaging data breaches.

[25] Davey Winder, Hacker Gives Away 386 Million Stolen Records on Dark Web—What You Need To Do Now, Forbes (July 29, 2020), available at https://www.forbes.com/sites/daveywinder/2020/07/29/hacker-gives-away-386-million-stolen-records-on-dark-web-what-you-need-to-do-now-shinyhunters-data-breach/ (last visited Mar. 2, 2026).

[26] ShinyHunters Offers Stolen Data on Dark Web, DarkReading (July 28, 2020), available at https://www.darkreading.com/cyberattacks-data-breaches/shinyhunters-offers-stolen-data-on-dark-web (last visited Mar. 2, 2026).

76. ShinyHunters is known for its financially motivated operations, primarily involving the theft and sale of data. They have compromised several companies, such as PowerSchool, Pixlr, NitroPDF, and MeetMindful, often leaking the stolen data on hacking forums either for free or for sale.

77. ShinyHunters aims to collect mass amounts of PII and PHI and has disseminated data for sale through a variety of dark web forums. These forums have, at times, been shut down by the FBI, only to reemerge with a different dark web address.[27]

78. ShinyHunters is known for targeting companies with large user bases, like Mercer. The group exfiltrates data from these organizations and extorts data breach victims to pay exorbitant sums or risk their data being sold on the dark web.

79. ShinyHunters has targeted well-known platforms and services, typically those with weaker security measures, large user databases, or high-profile reputations.

80. In some instances, ShinyHunters engages in ransom-based attacks, demanding payments to avoid leaking stolen data. Unlike other groups that specialize in ransomware or advanced persistent threat tactics, ShinyHunters focuses on maximizing the volume of data they acquire and monetize.

81. According to Skyhigh Security,[28] the typical ShinyHunters modus operandi includes:

---

[27] Jai Vijayan, Leak Site BreachForums Springs Back to Life Weeks After FBI Takedown, DarkReading (May 29, 2024), available at https://www.darkreading.com/cyberattacks-data-breaches/leak-site-breachforums-springs-back-to-life-weeks-after-fbi-takedown (last visited Mar. 2, 2026).

[28] Rodman Ramezanian, Ticketmaster's Encore: How "ShinyHunters" Hacked the Show, Skyhigh Security (July 11, 2024), available at

- **Orchestrating deception campaigns** by deploying sophisticated phishing schemes that aim to lure victims with fraudulent emails to capture login credentials.
- **Targeting unsecured cloud storage** to capitalize on poorly protected online storage data, which is akin to raining unguarded digital vaults**.**
- **Infiltrating and compromising web platforms and development tools,** often purloining login details or application programming interface (API) keys to pilfer valuable data.
- **Probing GitHub repositories** to scrutinize company code repositories for exploitable flaws, potentially granting unauthorized database access.
- **Monetizing via covert networks** to profit by trading stolen data on obscure internet marketplaces,catering to buyer seeking illicit information.

82. ShinyHunters also has a history of actually using the data it acquires, not just selling or threatening to sell it. For example, after ShinyHunters hacked Ticketmaster, the group announced that it possessed barcodes for entry to Taylor Swift's Eras tour and "an additional 30 million barcodes for other high-profile concerts and sporting events."[29]

83. ShinyHunters often targets applications with weak API security, including applications that lack multifactor authentication or rate-limiting. By exploiting these weaknesses, they can access sensitive data through exposed API endpoints. Once they gain access to an organization's database, ShinyHunters uses APIs to retrieve sensitive data in bulk.

84. ShinyHunters is active on the dark web, where the group lists data breaches for sale. It typically offers "exclusive" sales, where only one buyer receives the dataset, or "multi-

---

https://www.skyhighsecurity.com/about/resources/intelligence-digest/ticketmasters-encore-how-shinyhunters-hacked-the-show.html (last visited Mar. 2, 2026).

[29] Nick Robins-Early, Hackers leak alleged Taylor Swift ticket data to extort Ticketmaster, The Guardian (July 5, 2024), available at https://www.theguardian.com/us-news/article/2024/jul/05/taylor-swift-eras-tour-ticketmaster-hack-ransom (last visited Mar. 2, 2026).

buy" options, where the dataset is sold to several buyers. The group has carefully cultivated a reputation on forums, which makes buyers more likely to trust and purchase the listings. The group provides "sample" data from breaches to verify authenticity, encouraging purchases by demonstrating the quality of data.

85. ShinyHunters also occasionally "leaks" data in a staged manner to maximize pressure on the victim. The group sometimes releases partial data as a warning, then gives targets a chance to pay before the full release.

86. ShinyHunters has listed data for sale on the dark web even if a ransom is paid. ShinyHunters, for example, hacked AT&T in April 2024, obtaining some 86 million customer records, including customers' SSNs, mailing addresses, and dates of birth.[30] It was reported in July 2024 that AT&T paid ShinyHunters around $370,000 to delete this data.[31] Despite this ransom payment, this data was re-packaged and re-uploaded to a popular Russian cybercrime forum in 2025.[32]

87. ShinyHunters often begins by searching for companies using Microsoft Office 365 and third parties that store GitHub open authorizations tokens.[33] The group then identifies

[30] Christianna Silva, Hackers leak 86 million AT&T customer records with 44 million social security numbers, report says, Mashable (June 6, 2025), available at https://mashable.com/article/leaked-att-customer-record-social-security-numbers (last visited Mar. 2, 2026).

[31] Kim Zetter, AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records, WIRED (July 14, 2024), available at https://www.wired.com/story/atandt-paid-hacker-300000-to-delete-stolen-call-records/ (last visited Mar. 2, 2026).

[32] Chris Riotta, AT&T Hit by Massive Reported Identity Data Leak – Again, Bank Info Security (June 5, 2025), available at https://www.bankinfosecurity.com/att-hit-by-massive-reported-identity-data-leak-again-a-28595 (last visited Mar. 2, 2026).

[33] Researchers Share Common Tactics of ShinHunters Threat Group, DarkReading (Aug. 24, 2021) available at https://www.darkreading.com/cyberattacks-data-breaches/researchers-share-common-tactics-of-shinyhunters-threat-group (last visited Mar. 2, 2026).

research, development, and other employees with broad access to data in the organizations. ShinyHunters also has a history of attacking developer repositories to steal credentials or API keys.[34]

88. In sum, ShinyHunters is a notorious, decentralized hacking group whose tactics are well-known and foreseeable.

I. Defendant Breached a Duty of Care Owed to Plaintiff and Class Members Resulting in Injury.

89. Plaintiff's and Class Members' PII was stored on Defendant's platforms, networks, systems or products at the time of the Data Breach.

90. Defendant owed common law duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

91. At the time of the Data Breach, Mercer failed to maintain reasonable data security measures and comply with FTC guidance and other relevant industry standards.

92. Mercer' data security failings enabled the Data Breach. Without these basic protections, cybercriminals were able to exfiltrate Plaintiff's and Class Members' PII.

93. Mercer, through these data security failings, breached its express representations in its Privacy Policy which are detailed earlier in the complaint.

[34] Ravie Lakshmanan, Researchers Detail Modus Operandi of ShinyHunters Cyber Crime Group, The Hacker News (Aug. 23, 2021), available at https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html (last visited Mar. 2, 2026).

94. Alternatively, Mercer breached implied commitments to protect the PII of customers and employees, including Plaintiff and Class Members, by virtue of mandating that customers and employees provide their sensitive PII as a condition of using or purchasing Mercer's products and services and/or being employed by Mercer.

95. Mercer's basic data security shortcomings also constitute a breach of their duty of care to protect the PII of customers and employees, including Plaintiff and Class Members.

96. Mercer's data security failings also constitute an unfair trade practice. As discussed above, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of PII violates the FTC Act's prohibition on "unfair and deceptive acts."

97. Mercer's breach of its duty of care and engagement in unfair trade practices caused injury to Plaintiff and Class Members.

98. Mercer is liable for the injuries suffered by Plaintiff and Class Members by virtue of its role in the collection, transfer of and storage of the data of its affected customers.

99. Plaintiff and Class Members have and will continue to suffer the following forms of injury fairly traceable to the Data Breach.

100. The Data Breach's disclosure of Plaintiff's and Class Members' PII has created a substantial risk that their data will be misused. That cybercriminals now control that data demonstrates this risk.

101. Plaintiff and Class Members have and will continue to reasonably expend significant time and costs mitigating the substantial risk of data misuse. These mitigation steps include Plaintiff and Class Members now expending time and effort to place "freezes" and

"alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

102. Plaintiff and Class Members have and may suffer lost property value of their PII when Defendant allowed their PII to fall into the hands of cybercriminals, who could—and likely will—freely sell or distribute it at any time.

103. Defendant breached its express and implied contractual commitments to Plaintiff and Class Members to protect their PII.

104. The breach of a contractual obligation constitutes an injury to Plaintiff and Class Members and provides a basis for a lawsuit to enforce the contractual terms.

105. In breaching its contractual commitments, Defendant further injured Plaintiff and Class Members by depriving them of the benefit of the bargain they had reached.

106. For example, Plaintiff and Class Members entered into agreements with Mercer based on express and implied representations that their PII would be protected—which they factored into the value of that exchange. By failing to maintain reasonable data security measures to protect that PII, Defendant deprived Plaintiff and Class Members of the benefit of the bargain by which it owed the value of reasonable data security measures that were not provided.

107. Plaintiff and Class Members have or may have been injured by an invasion of their privacy rights. The disclosure of their PII to cybercriminals and potentially others if and when the cybercriminals disclose it on the dark web involves PII whose private nature was compromised by the Data Breach.

108. In addition, Plaintiff and Class Members have or may suffer emotional distress and anxiety resulting from the Data Breach and fear the substantial risk of identity theft and loss of privacy. Plaintiff and Class Members understand that their PII cannot now be clawed back from the dark web.

J. Plaintiff Paul Berger's Experience

109. Plaintiff Paul Berger is a customer of Mercer financial planning and investment services.

110. In order to utilize Mercer's products and services, Plaintiff Berger was required to entrust Mercer with his PII.

111. Upon information and belief Mr. Berger's PII was stolen from Defendant's systems, networks, and/or software in the Data Breach.

112. Mercer possessed Mr. Berger's PII before, during, and after the Data Breach.

113. On February 25, 2026, Plaintiff received notice from Mercer that it had recently identified unauthorized access to some of its systems used to store client data and to be cautious of unsolicited emails or phone calls that ask for personal information or ask you to send money.

114. Because of the Data Breach, Mr. Berger's confidential PII is in the hands of cybercriminals. As such, Mr. Berger and other Class Members are at imminent risk of identity theft and fraud.

115. As a result of the Data Breach, Mr. Berger must expend hours of his time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best

to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

116. Mr. Berger places significant value on the security of his PII and does not readily disclose it. Mr. Berger has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

117. Mr. Berger has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

118. Mr. Berger has a continuing interest in ensuring that his PII—which, upon information and belief, remains in the possession of Mercer—is protected, and safeguarded from future data breaches. Absent court intervention, Mr. Berger's and Class Members' PII will be wholly unprotected and at-risk of future data breaches.

119. Mr. Berger suffered actual injury as a result of the unauthorized access and disclosure of his PII in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of his PII; (iii) lost or diminished value of his PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Mercer' possession and is subject to further unauthorized disclosures so long as Mercer fails to undertake appropriate and adequate measures to protect his PII.

120. The Data Breach caused Mr. Berger to suffer fear, anxiety, and stress, which has been compounded by the fact that Mercer has still not informed him of key details about the Data Breach.

K. Plaintiff and Class Members Suffered Damages

121. Given the sensitivity of the PII involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Mercer has done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Mercer has not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach.

122. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

123. Since learning of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

124. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

125. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

126. As a direct and proximate result of Mercer's conduct, Plaintiff and Class members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

127. As a direct and proximate result of Mercer's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

128. Plaintiff and Class Members 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.

129. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

130. 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.

131. 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 similar cases.

132. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Mercer was intended to be used by Mercer to fund adequate

security of its computer system(s) and Plaintiff's and Class Members' PII. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

133. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

134. 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 relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

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

135. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in Mercer's possession, 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 Private Information is not accessible online and that access to such data is password protected.

136. Further, as a result of Mercer's conduct, Plaintiff 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.

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

V. CLASS ACTION ALLEGATIONS

138. Plaintiff brings this nationwide class action on behalf of himself and all others similarly situated pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

139. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach (the "Class").

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

141. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

142. **Numerosity.** The Class described above is 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 Mercer's records, including, but not limited to, the files implicated in the Data Breach. Upon information and belief, the Class, at minimum, comprises well over a million individuals.

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

- whether and to what extent Mercer had a duty to protect the PII of Plaintiff and Class members;
- whether Mercer was negligent in collecting and storing Plaintiff's and Class members' PII;
- whether Mercer had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;
- whether Mercer took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
- whether Mercer failed to adequately safeguard the PII of Plaintiff and Class members;
- whether Mercer breached its duties to exercise reasonable care in handling Plaintiff's and Class members' PII;
- whether Mercer failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- whether Plaintiff and Class members are entitled to damages as a result of Mercer's wrongful conduct; and
- whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

144. **Typicality.** Plaintiff's claims are typical of the claims of the Class members. The claims of Plaintiff and Class members are based on the same legal theories and arise from the

same failure by Mercer to safeguard their PII. Plaintiff and Class Members entrusted Mercer with their PII, and it was subsequently accessed by an unauthorized third party.

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

146. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the proposed Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

147. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Mercer's liability and the fact of damages is common to Plaintiff and each member of the

proposed Class. If Mercer breached its duties and released Plaintiff's and Class Members' PII, then Plaintiff and each Class member suffered damages by that conduct.

148. **Ascertainability:** Members of the proposed Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Mercer's books and records.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

149. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

150. Mercer owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Mercer's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

151. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Mercer's cloud-based systems to ensure that Plaintiff's and Class Members' PII in Mercer's possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

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

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

154. Mercer also owed a common law duty to Plaintiff and Class Members because their conduct created a foreseeable risk of harm to them. Mercer's conduct included their failure to adequately restrict access to their computer networks and/or servers that held individuals' PII.

155. Mercer also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyber-attacks, such as the Data Breach..

156. Mercer breached the duties owed to Plaintiff and Class Members and thus were negligent. Mercer breached these duties by, among other things: (a) mismanaging their 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 their data security by failing to assess the sufficiency of their 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 their 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; (g) failing to follow their own privacy policies provided to customers; and (h) failing to adequately train and supervise

employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

157. But for Mercer's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII would not have been accessed, exfiltrated, and compromised by cybercriminals.

158. As a direct and proximate result of Mercer's negligence, Plaintiff and Class Members have suffered injuries including:

a. theft of their PII;

b. costs associated with requesting credit freezes;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. 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 Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. damages to and diminution in value of their PII entrusted to Mercer with the mutual understanding that Mercer would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

i. continued risk of exposure to hackers and thieves of their PII, which remains in Mercer's possession and is subject to further breaches so long as Mercer fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

159. As a direct and proximate result of Mercer's negligence, including their gross negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

160. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

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 companies such as Mercer for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Mercer's duties.

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

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

164. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

165. Mercer's violation of Section 5 of the FTC Act constitutes negligence *per se*.

166. As a direct and proximate result of Mercer's negligence, Plaintiff and Class members have suffered injuries, including those identified in Paragraph 91 above.

167. As a direct and proximate result of Mercer's negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

168. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

169. Plaintiff and Class members conferred a monetary benefit on Mercer by providing them with their valuable PII.

170. Mercer knew that Plaintiff and Class members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to them. Mercer profited from Plaintiff's and Class members' PII and use of Plaintiff' and Class members' PII for business purposes.

171. Mercer failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

172. Mercer acquired the PII through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

173. If Plaintiff and Class members had known Mercer would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Mercer.

174. Under the circumstances, it would be unjust for Mercer to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon them.

175. Plaintiff and Class members are without an adequate remedy at law.

176. As a direct and proximate result of Mercer's conduct, Plaintiff and Class members have suffered injuries, including those identified above.

177. Plaintiff and Class members are entitled to restitution and/or damages from Mercer and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Mercer from their wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

FOURTH CLAIM FOR RELIEF
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

178. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

179. Plaintiff and the Class entrusted their Private Information to Mercer as a condition of purchasing products and obtaining services. In so doing, Plaintiff and the Class entered into implied contracts with Mercer, pursuant to which Mercer agreed to safeguard and protect Plaintiff's and Class members' Private Information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached, compromised, or stolen.

180. At the time Mercer acquired the Private Information of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Mercer would safeguard the Private Information and not take unjustified risks when storing the Private Information.

181. Implicit in the agreements between Plaintiff and Class members and Mercer was Mercer's obligation to: (a) use Plaintiff and Class members' Private Information for business purposes only; (b) take reasonable steps to safeguard their Private Information; (c) prevent unauthorized access and disclosure of the Private Information; (d) provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; and (e) retain the Private Information only under conditions that kept such information secure and confidential.

182. Plaintiff and the Class would not have entrusted their Private Information to Mercer had they known that Mercer would not encrypt sensitive data elements, or delete the Private Information that Mercer no longer had a reasonable need to maintain.

183. Plaintiff and the Class fully performed their obligations under the implied contracts with Mercer.

184. Mercer breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their Private Information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that their Private Information had been compromised and stolen in the Data Breach.

185. As a direct and proximate result of Mercer's above-described breach of implied contract, Plaintiff and Class members have already suffered, and will continue to suffer, damages including, inter alia: (i) invasion of privacy; (ii) theft of their Private Information; (iii) actual and attempted misuse of the Private Information stolen in the Data Breach, including an increase in spam and phishing calls, texts, and emails; (iv) lost time, money, and opportunity costs associated with attempts to mitigate the actual consequences of the Data Breach; (v) lost or diminished value of their Private Information; (vi) loss of the benefit of their bargain; (vii) nominal damages; and (viii) the increased and continuing risk to their Private Information, which: (a) remains unencrypted and vulnerable to unauthorized access and abuse; and (b) remains backed up in Mercer's possession and is subject to further unauthorized disclosures so long as Mercer fails to undertake appropriate and adequate measures to protect the Private Information.

186. Plaintiff and the Class have suffered (and will continue to suffer): an ongoing and imminent threat of future identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual and attempted identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of their stolen Private Information; the illegal sale of the compromised data on the Dark Web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, lost work time; and other economic and non-economic harm.

187. As a direct and proximate result of Mercer's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial..

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, pray for relief as follows:

A. For an order certifying the proposed Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff' attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

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

H. Awarding such other and further relief as may be just and proper.

VIII. JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all claims so triable.

Dated: March 2, 2026

Respectfully submitted,

/s/Eric R. Olson
Eric R. Olson
OLSON GRIMSLEY KAWANABE HINCHCLIFF & MURRAY LLC
1700 17th Street, Suite1600
Denver, CO 80210
Telephone: 303-535-9151
Email: eric.olson@olsongrimsley.com

James J. Pizzirusso
Nicholas U. Murphy (admission forthcoming)
Kira Hessekiel (admission forthcoming)
HAUSFELD LLP

1200 17th Street, NW, Suite 600
Washington, DC 20036
Telephone: 202-540-7200
Email: jpizirusso@hausfeld.com
Email: nmurphy@hausfeld.com
Email: khessekiel@hausfeld.com

Steven M. Nathan (admission forthcoming)
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, New York 10004
Tel.: (646) 357-1100
Email: snathan@hausfeld.com

Linda P. Nussbaum (admission forthcoming)
NUSSBAUM LAW GROUP, P.C.
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Telephone: (917) 438-9189
Email: lnussbaum@nussbaumpc.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org