IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
CLEVELAND DIVISION

MICHAEL J. BROUTY, MELISSA D. KAUFFMAN, AND LEBERTUS VANDERWERFF *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

KEYBANK NATIONAL ASSOCIATION, KEYCORP, and OVERBY-SEAWELL COMPANY,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Page

Contents

CLASS ACTION COMPLAINT

Plaintiffs, identified in Section III.A. below, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendants KeyBank National Association ("KNA") and its bank holding company Keycorp (collectively, "Key"), and Overby-Seawell Company ("Overby-Seawell"), seeking monetary damages, restitution, and/or injunctive relief regarding Key's cybersecurity practices. Plaintiffs make the following allegations upon personal knowledge, information and belief derived from, among other things, investigation of their counsel and facts that are a matter of public record.

I. INTRODUCTION

1. This lawsuit exists because cybercriminals unsurprisingly targeted a company in the business of storing personal information, stealing valuable personal information, including customers' names, the first eight digits of customers' Social Security numbers, mortgage property addresses, phone numbers, property information, and other insurance and mortgage information which personally identifies the customer ("PII").

2. Overby-Seawell, which provides property-insurance verification services for Key, informed Key on August 4, 2022, that an unauthorized external party had gained remote access to OSC's network and, on July 5, 2022, acquired certain information from a number of OSC clients, including the PII of Key's customers (the "Data Breach").

3. For its part, Key is a mortgage lender and servicer that operates in fifteen states, and boasts $187 billion in assets.

4. The value of the PII stolen in this case is recognized by several different constituencies. First, the value is recognized by the Defendants, who can attribute their business models to the existence of this information, and the need to keep it safe. Second, the value is

recognized by cybercriminals, who know that this type of data can be exploited to commit identity theft. And third, the value is recognized by the individuals, themselves, whose PII was stolen.

5. Key identifies itself as the "[y]our local, responsible, award-winning bank"[1] and claims that it uses "[s]tate-of-the-art security to help protect our clients."[2] Key markets its expertise in safeguarding information to both consumers and corporate clients—not only because statutory schemes require certain levels of data security, but also to thwart cybersecurity attacks. Key claims that it "rel[ies] on advanced data protection, strong encryption and continual monitoring to protect your account."[3] However, the Data Breach has revealed that this is not the case.

6. Tens of thousands of individuals have shared their most valuable data with Key based on the ordinary, reasonable understanding that their information, much of it sensitive, would be handled and maintained with appropriate safety standards—the very services that Key boasts of in protecting its customers.

7. Despite Key's representations that it provided robust cybersecurity services, in reality, its security program (and that, in particular, of the agents to whom it entrusted information) was woefully inadequate. Key's and its agents' unsound, vulnerable systems containing valuable data were an open invitation for intrusion and exfiltration by cybercriminals, who were seeking to exploit the valuable nature of the information.

8. The unlawfully deficient data security employed by Key and its agents has injured tens of thousands of customers, the Plaintiffs and putative Class members in this action, and its

---

[1] *About Key, Company Information, Get to Know Key*, https://www.key.com/about/company-information/key-company-overview.html (last visited September 24, 2022).

[2] *About Key, Security, Banking Security*, https://www.key.com/about/security/privacy-security.html (last visited September 24, 2022).

[3] *About Key, Security, Online Banking Security and Fraud Protection*, https://www.key.com/about/security/consumer-security.html (last accessed September 26, 2022).

failure to connect any fraudulent activity that its customers have faced with the Data Breach reeks of a desire to avoid responsibility.

II. NATURE OF THE ACTION

9. Key describes itself as "one of the nation's largest, bank-based financial services companies" with approximately 1,000 service branches in fifteen states, and over $187 billion in assets.[4] Key provides banking services in two tranches: consumer, and commercial.

10. The Consumer Bank serves individuals and small businesses through local branches and through its national Laurel Road digital lending business "by offering a variety of deposit and investment products, personal finance and financial wellness services, lending, student loan refinancing, mortgage and home equity, credit card, treasury services, and business advisory services."[5] In addition, Key's consumer banking offers wealth management and investment services for nonprofits and high-net-worth clients, and assists with their banking, trust, portfolio management, charitable giving, and related needs.[6]

11. The commercial side of Key is a full-service corporate bank focused principally on serving the needs of middle market clients in seven industry sectors: consumer, energy, healthcare, industrial, public sector, real estate, and technology. The Commercial operating segment is also a significant servicer of commercial mortgage loans and a significant special servicer of commercial-backed mortgage security.[7]

12. Plaintiffs, and the other Class members, are customers of Key's consumer banking side.

---

[4] *Get to Know Key*, https://www.key.com/about/company-information/key-company-overview.html (last accessed September 26, 2022).
[5] *Id.*
[6] *Id.*
[7] *Id.*

13. According to KeyCorp's 2022 10-K, the "largest segment of [Key's] consumer loan portfolio" is the "residential mortgage portfolio", which is comprised of loans originated by the Consumer Bank, and represents approximately 51% of consumer loans held by Key. This is followed by Key's home equity portfolio, which is comprised of approximately 27% of consumer loans outstanding at year end.[8]

14. Key knew that the information provided to it by its mortgage customers contained some of the Plaintiffs' and Class members' most valuable personal information, and that such information would make any entity that stored it an attractive target for cybercrime.

15. Key then gave this sensitive information to its agent, Overby-Seawell Company ("OSC"), which used the information for the purposes providing Key with ongoing mortgage insurance verification for Key's residential mortgage clients.

16. Key utterly failed to properly evaluate and audit its agent to whom it entrusted this most sensitive of personal information.

17. Key acknowledged in its 2022 SEC filing that a "technology failure, cyberattack or other security breach that significantly compromises the systems of one or more financial parties or service providers could have a material impact on counterparties or market participants, including us. Any third-party technology failure, cyberattack, or security breach could adversely affect our ability to effect transactions, service clients, or otherwise operate our business."[9] Nevertheless, it failed to heed its own warnings.

18. Sophisticated companies like Key are aware of the different types of threat actors acting across the internet and the type of security exploits they employ for profit. Accordingly,

[8] Form 10-K filed with the SEC on February 22, 2022.

[9] *Id.*

Key understood that it was imperative to guard against those exploits and ensure that the third-party contractors it employs as agents adopt adequate security measures as well.

19. The release, disclosure, and publication of a person's sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is also a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[10] A data breach can have grave consequences for victims for many years after the actual date of the breach—with the obtained information, identity thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, file false tax returns, or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

20. Nevertheless, in August 2022, Key failed to oversee and require that OSC maintain adequate cybersecurity protections, and, as a result, OSC "suffered a cybersecurity incident that compromised data of its corporate clients, including personal information associated with KeyBank mortgage clients."[11]

21. Had Key maintained a sufficient security program, and required that its third-party agents and vendors do so as well, it would have discovered the cyberattack sooner or prevented it altogether.

22. Plaintiffs' PII has been compromised and disclosed to unauthorized third parties because of Key and OSC's joint negligent and unlawful conduct—the PII that Key collected and

[10] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, 29-35, 30 S.C. Lawyer (May 2014), https://mydigitalpublication.com/publication/?m=18928&i=208503&p=1&ver=html5 [https://perma.cc/L3KT-VQXC].

[11] Lauren Talotta, *KeyBank customers information possibly at risk after third-party data breach*, Sept. 3, 2022 (available at https://www.wpxi.com/news/local/keybank-hackers-third-party-provider-stole-customer-data/XIORXKWUPZEKXPEYGGMJZR2CRQ/).

OSC maintained is now in the hands of cybercriminals. In fact, the Notices Key has provided to its customers advise that Plaintiffs and Class members should remain aware of suspicious account activity, recognize, avoid and report common fraud attempts by phone, email and text, take further actions such as monitoring their own credit records, and notify the organizations involved and law enforcement authorities of any suspicious activity. Despite this, Defendants offered Class members little in the way of redress, such as credit monitoring or fraud protection, and provided no financial support for time or expenses incurred as a result of the Data Breach.

23. As a result of the Data Breach, Plaintiffs and the Class members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud, identity theft, and ransom demands for many years to come. Furthermore, Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft at their own expense. Consequently, Plaintiffs and the Class members will incur ongoing out-of-pocket costs including the cost of credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft, among other expenses.

24. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was compromised and disclosed as a result of the Data Breach.

25. Accordingly, Plaintiffs bring this action against Defendants seeking redress for their unlawful conduct, and asserting claims for both common law and statutory damages.

III. PARTIES

A. Plaintiffs

26. Plaintiffs identified below bring this action on behalf of themselves and those similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, Defendants, through their actions described

herein, leaked, disbursed, and furnished Plaintiffs' valuable PII to unknown cybercriminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

27. As used throughout this Complaint and previously defined in paragraph1, "PII" is further defined as all information exposed by the Data Breach, including all or any part or combination of name, address, birth date, SSN, , driver's license information (including license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or dispute documents with PII (such as images of government-issued identifications).

28. Plaintiff Melissa D. Kauffman is a resident and citizen of Indiana. Plaintiff Kauffman is acting on her own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff Kauffman's PII, and have a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Kauffman would not have entrusted her PII to Defendants had she known that the Defendants' failed to maintain adequate data security. Plaintiff Kauffman's PII was compromised and disclosed as a result of the Data Breach.

29. Plaintiff Kauffman received notice from Key that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Kauffman's PII, including full name, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, the first eight digits of her social security number, home insurance policy number, and home insurance information was compromised as a result of the Data Breach.

30. As a result of the Data Breach, Plaintiff Kauffman made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching

the Data Breach and Defendants; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud and freezing her credit.

31. As a result of the Data Breach, Plaintiff Kauffman has suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Kauffman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

32. Plaintiff Kauffman suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) loss of the value of her PII, a form of property that Defendants obtained from Plaintiff Kauffman; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

33. As a result of the Data Breach, Plaintiff Kauffman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Kauffman will continue to be at increased risk of identity theft and fraud for years to come.

34. Plaintiff Michael James Brouty is a resident and citizen of New York. Plaintiff Brouty is acting on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff Brouty's PII, and have a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Brouty would not have entrusted his PII to Defendants had he known that the Defendants failed to maintain adequate data security. Plaintiff Brouty's PII was compromised and disclosed as a result of the Data Breach.

35. Plaintiff Brouty received notice from Key that his PII had been improperly accessed and/or obtained by unauthorized third parties upon logging into his KeyBank portal. This notice indicated that Plaintiff Brouty's PII, including full name, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, the first eight digits of his social security number, home insurance policy number, and home insurance information were compromised as a result of the Data Breach.

36. As a result of the Data Breach, Plaintiff Brouty made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to reviewing his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Brouty now spends approximately 7-8 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities, significantly more than he spent prior to the Data Breach.

37. Plaintiff Brouty does not recall if he was offered credit monitoring and identity theft protection services by the Defendants.

38. As a result of the Data Breach, Plaintiff Brouty has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Brouty is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

39. Plaintiff Brouty suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) loss of the value of his PII, a form of property that Defendants obtained from Plaintiff Brouty; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

40. As a result of the Data Breach, Plaintiff Brouty anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Brouty will continue to be at increased risk of identity theft and fraud for years to come.

41. Plaintiff Lebertus Vanderwerff is a resident and citizen of New York. Plaintiff Vanderwerff is acting on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff Vanderwerff's PII, and have a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Vanderwerff would not have entrusted his PII to Defendants had he known that the Defendants failed to maintain adequate data security. Plaintiff Vanderwerff's PII was compromised and disclosed as a result of the Data Breach.

42. Plaintiff Vanderwerff received notice by mail from Key that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Vanderwerff's PII, including full name, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, the first eight digits of his social security number, home insurance policy number, and home insurance information were compromised as a result of the Data Breach, and told him only that he should monitor his credit score with the three major credit ratings agencies, but did not offer any credit monitoring services, or identity theft protections services.

43. As a result of the Data Breach, Plaintiff Vanderwerff made reasonable efforts to mitigate its impact after receiving the notification letter, including reviewing credit reports 3-4 times weekly for a few hours at a time, as well as monitoring his financial account statements for any indications of actual or attempted identity theft or fraud and freezing his credit. This regular

review revealed that one of Plaintiff Vanderwerff's business accounts was breached, and used to make a $600 fraudulent charge at a guitar shop in California shortly after he was notified of the Data Breach.

44. As a result of the Data Breach, Plaintiff Vanderwerff has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Vanderwerff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

45. Plaintiff Vanderwerff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) loss of the value of his PII, a form of property that Defendants obtained from Plaintiff Vanderwerff; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

46. As a result of the Data Breach, Plaintiff Vanderwerff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Vanderwerff will continue to be at increased risk of identity theft and fraud for years to come.

B. Defendant

47. Defendant KeyBank National Association is organized under the laws of the United States, and maintains its principal place of business in Cleveland, Ohio. Among other things, KeyBank originates and periodically sells commercial and residential mortgage loans but continues to service those loans for the buyers of those mortgages.

48. Defendant Keycorp is a Fortune 500 publicly-traded company incorporated in Ohio with a principal place of business in Cleveland, Ohio. KeyCorp is a bank holding company

("BHC") under the Bank Holding Company Act of 1956. KeyCorp is the parent holding company for KeyBank, its principal subsidiary. KeyBank operates in 15 states.

49. Defendant Overby-Seawell Company ("OSC") is incorporated in Georgia, and maintains its principal place of business in Kennesaw, Georgia. OSC is a technology services vendor that provides ongoing verification for KeyBank's residential mortgage clients' maintenance of property insurance, which are required for homeowners to maintain based on the terms of the mortgage.

IV. JURISDICTION AND VENUE

50. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than the Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

51. This Court has personal jurisdiction over Key because KNA and Keycorp maintain their principal places of business in this District, have sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

52. This Court has personal jurisdiction over OSC because OSC has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

53. This Court also has diversity jurisdiction over this action. *See* 28 U.S.C. § 1332(a).

54. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because two of the Defendants' principal places of business are located in this District and a substantial part of

the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

V. STATEMENT OF FACTS

A. The Data Breach

55. On July 5, 2022, an "unauthorized external party" gained remote access to OSC's network, acquired certain information from a number of OSC's clients, including certain personal information of Key's customers.

56. This PII included names, mortgage property addresses, mortgage account numbers and mortgage account information, phone numbers, property information, the first eight digits of Social Security numbers, and home insurance policy number and home insurance information ("PII") belonging to Plaintiffs and Class Members.

57. Plaintiffs' PII was part of the data acquired by unauthorized third parties from OSC's systems in the Data Breach.

58. Key issued a Notice on July 26, 2022, informing its customers of the occurrence of the Data Breach, as well as the categories of PII which were exposed in the Data Breach.

59. The Notice issued, sent, or otherwise made available to Plaintiffs stated that OSC was investigating the incident with the assistance of third-party cybersecurity experts, as well as the Federal Bureau of Investigation.

60. Upon information and belief, the Defendants' internal investigation, and the investigation being conducted by the FBI, are not yet complete.

61. As a result, the categories of PII listed in the Notice as having been acquired by an unauthorized third party may not be a complete list of the PII exposed in the Data Breach.

62. The Notice also stated that OSC has deployed enhanced security monitoring tools across their network in response to the Data Breach.

63. Upon information and belief, these security monitoring tools were available to OSC prior to the Data Breach.

64. The Notice also recommends that affected customers obtain credit monitoring and identity theft protection services to help them detect possible fraud or misuse of their PII, and indicated that Key would provide such credit monitoring and identity theft protection for two years.

65. Since the initial Notice sent out to customers in late July, none of the Defendants have offered further updates on the results of their investigations, or potential misuse of PII.

B. Defendants' Responsibility to Safeguard Information

66. Beyond the obligations created in their security and privacy policies, Defendants owed Plaintiffs and Class members a duty to safeguard their Private Information.

67. First, as described further below, Defendants owed a duty to safeguard Private Information pursuant to a number of statutes, including the Federal Trade Commission Act ("FTC Act"), to ensure that all information they collected and stored was secure. These statutes were intended to protect Plaintiffs and the Class members from the type of conduct by Defendants alleged herein.

68. Next, Defendants owed a duty to safeguard Private Information given that they were on notice that they were maintaining highly valuable data, for which Defendants knew there was a risk that they would be targeted by cybercriminals. Defendants knew of the extensive harm that would occur if Plaintiffs' and Class members' Private Information was exposed through a Data Breach, and thus owed a duty to safeguard that information.

69. Given the sensitive nature of the Private Information obtained by Defendants, they knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially engineered attacks, healthcare fraud, and other identity-related fraud if they were able to exfiltrate that data from Defendants' servers. Defendants also knew that individuals whose

Private Information was stored on their servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

70. Defendants also owed a duty to safeguard Plaintiffs' and Class members' data based upon the promises that they made to their customers to safeguard data, as well as the disclosures that they made in their data security policies and privacy policies. Defendants voluntarily undertook efforts to keep that data secure as part of their business model and thus owe a continuing obligation to Plaintiffs and Class members to keep their Private Information secure.

71. Defendants also owed a duty to comply with industry standards in safeguarding Private Information, which—as discussed herein—they did not do.

C. Defendants Failed to Meet Their Obligations to Protect Private Information or Comply with Their Own Privacy Policies

72. Defendants' services are supported by privacy policies and security practices, which they provide on their publicly facing websites.

73. Defendants were keenly aware of the obligations that state and federal law imposed upon them given the types of information that they obtained and stored from Key's mortgage customers.[12]

74. Defendants also had a special relationship with Plaintiffs and Class members from being entrusted with their Private Information, which provided an independent duty of care. Defendants had a duty to use reasonable security measures because they undertook to collect, store and use consumers' Private Information. In addition, Key had a duty to require that OSC would use reasonable security measures because it disclosed that same Private Information to OSC.

[12] *See* Key's Consumer Security page, available at https://www.key.com/about/security/consumer-security.html (last accessed September 26, 2022); *see also* OSC's Privacy Policy, available at https://www.oscis.com/privacy/ (last accessed September 26, 2022).

75. Accordingly, Defendants are liable to Plaintiffs and the Class for the compromise and unauthorized disclosure of their Private Information.

D. Defendants Failed to Comply with Industry and Regulatory Standards

76. Because of the value of PII to hackers and identity thieves, companies in the business of obtaining, storing, maintaining and securing Private Information, such as Defendants, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting 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.[13] Organizations, companies, and banks like Defendants have an added incentive to harden their networks against unauthorized penetration, because they directly control the data necessary to access consumers' financial accounts.

77. Further, federal and state governments have likewise established security standards and issued recommendations to reduce the number and size of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[14]

---

[13] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/ [https://perma.cc/NY6X-TFUY].

[14] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

78. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[15] The guidelines note businesses should protect the personal customer and consumer 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 security problems.[16] 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.[17]

79. The FTC recommends that companies 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 (most pertinent here) verify that third-party service providers have implemented reasonable security measures.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer 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 FTC Act, 15 U.S.C. § 45.

---

[15] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business [https://perma.cc/9945-U4HV].

[16] *Id.*

[17] *Id.*

Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

81. Defendants also have obligations created by other federal and state laws and regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Plaintiffs' and Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

82. Given the magnitude of the risk and repercussions of a breach or attack targeting this type of data, the likelihood of a breach or attack, and Defendant's explicit awareness of these vulnerabilities, Defendants should have taken every reasonable precaution in developing a robust security program and protecting Plaintiffs' and the Class members' Private Information.

83. Yet, despite its duties, representations, and promises, Defendants failed to adequately secure and protect their customers' data, allowing the Plaintiffs' and Class members' Private Information to be accessed, disclosed, and misused.

E. Data Breaches Put Consumers at Increased Risk of Fraud and Identify Theft

84. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Alphabet Inc., the parent company of Google, aptly illustrated this in its 2020 Annual Report, when it reported a total annual revenue of $182.5 billion and net income of $40.2 billion.[18] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about the users of its various free products and services. America's largest corporations

[18] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

profit almost exclusively through the use of Private Information illustrating the considerable market value of personal Private Information.

85. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

86. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

87. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

88. For example, in 2019, both Microsoft and Google have publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable

SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"[19] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

89. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[20]

90. Cyberattacks have become so notorious that the FBI and Secret Service issued an unprecedented warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[21]

91. Cyberattacks and data breaches of financial services companies are especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[22]

---

[19] Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW]. Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW].

[20] *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks [https://perma.cc/RKT2-LX5Z].

[21] Kochman, *supra* n.171.

[22] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/

92. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23]

93. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), 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.[24]

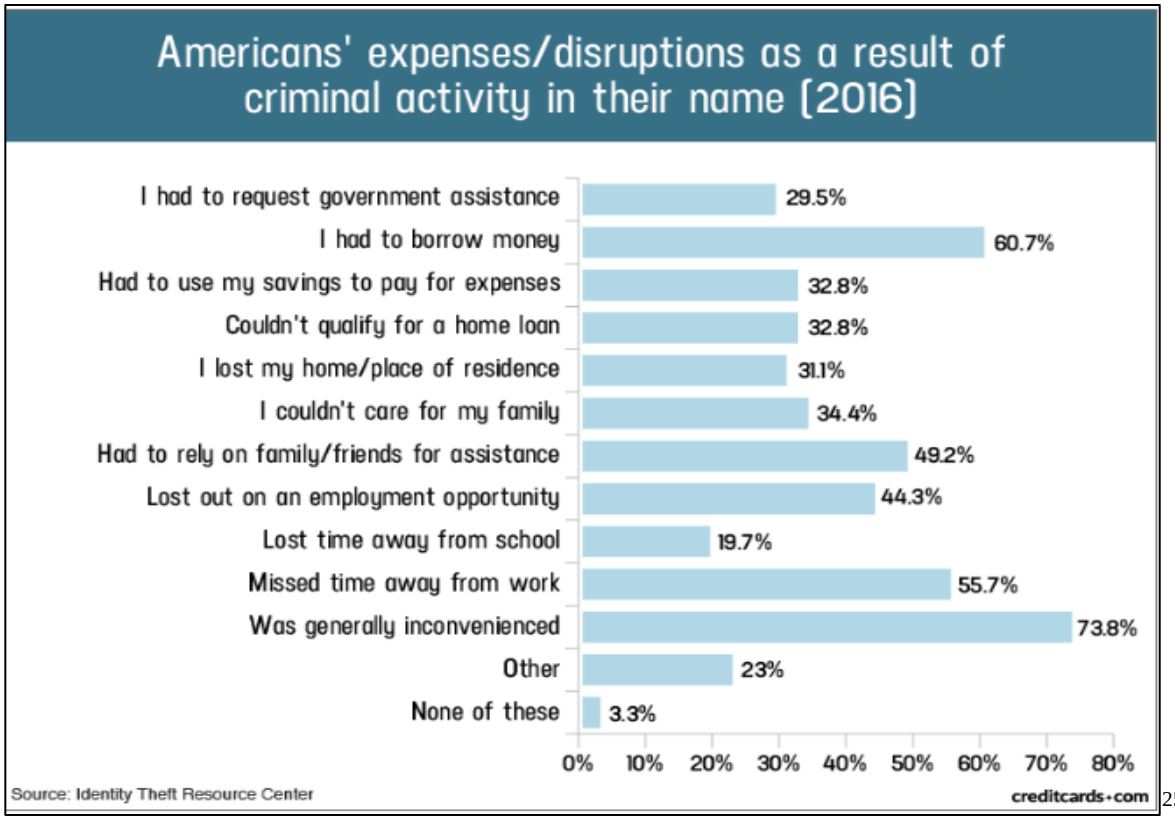
94. Cybercriminals use stolen Private Information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

95. Identity thieves can also use SSNs to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:

---

[23] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[24] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Mar. 23, 2021) [https://perma.cc/ME45-5N3A].



[25]

96. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[26] As illustrated in the above graphic, this includes devastating results such as "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.[27] The ITRC study concludes

[25] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

[26] *Id.*

[27] *Id.*

that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[28]

97. Private Information is a valuable property right.[29] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that the control over Private Information has considerable market value that is lost when it is compromised.

98. 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. According to the GAO, 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.[30]

Private Information is such an inherently valuable commodity to identity thieves that, once compromised, criminals often trade the information on the cyber black-market for years.

99. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase

---

[28] *Id.*

[29] *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 *1 (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.").

[30] GAO Report, *supra* n.23, at 29.

the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[31]

100. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and the Class members are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Plaintiffs and many of the Class members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Notices advise, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

VI. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES

101. Plaintiffs and Class members have been harmed and incurred damages as a result of the compromise of their Private Information in the Data Breach. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May of 2020, Plaintiffs did not receive Notice until July of 2020 at the earliest—*nearly six months after the breach began*.

A. Plaintiffs' and Class Members' Private Information was Compromised in the Data Breach

102. This Data Breach is not limited to automated attacks against the availability of information in Defendants' possession, custody or control. This incident included unauthorized

[31] *See* Kelion & Tidy, *supra* n.**Error! Bookmark not defined.** (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

persons taking possession of the information, available for their use however and whenever they see fit.

103. Plaintiffs were required to provide their Private Information, which was obtained and maintained by Defendants, and which Defendants had a duty to secure and safeguard.

104. Like Plaintiffs, the Class members' Private Information was compromised as a direct and proximate result of the Data Breach.

105. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class members have been damaged because of the disclosure of their Private Information in several ways.

106. First, Plaintiffs and Class members now suffer the very real and imminent threat of identity theft, evidenced by the notices received by the Plaintiffs, which advised Plaintiffs to remain vigilant, monitor their credit, and engage in preventative measures to avoid identity theft.

107. Second, Plaintiffs and Class members have sustained injuries as a result of the disclosure of their Private Information to unauthorized third-party cybercriminals as a result of Defendants' insufficient cybersecurity. As a result, Plaintiffs and Class members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and the Class members also face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class members have and will continue to incur out-of-pocket costs for protective measures such as on-going credit monitoring fees and may also incur additional costs for credit report fees, and similar costs directly

related to the Data Breach. Plaintiffs and the Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs and the Class members have and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

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

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

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

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

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

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

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

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

k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

108. Further, Plaintiffs and Class members will have to continue to spend significant amounts of time to respond to the Data Breach and monitor their financial, student, and medical accounts and records for misuse.

109. Third, Plaintiffs have, at the very least, sustained nominal damages for Defendants' violations as discussed herein. As a result of Defendants' failures to safeguard Plaintiffs' and the Class members' Private Information, they are forced to live with the knowledge that their Private Information—which contains private and personal details of their life—may be disclosed to the

entire world, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiffs and the Class members of their fundamental right to privacy.

110. Fourth, Plaintiffs are entitled to statutory damages, as provided, based upon the relevant causes of action alleged herein, and described below.

111. Fifth, Defendants benefitted at the expense of, and to the detriment of, Plaintiffs and Class members. Among other things, Defendants continue to benefit and profit from Class members' Private Information while its value to Plaintiffs and Class and Subclasses members has been lost.

112. Finally, Plaintiffs and the Class members have an interest in ensuring that their Private Information, which remains in the possession of the 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 Plaintiffs' and the Class members' data is not accessible online and that access to such data is limited and secured.

113. Defendants' actions causing the Data Breach, and their failure to provide complete and accurate information to Plaintiffs, Class members, government officials, and the general public about the Data Breach; harms not only Plaintiffs and Class members but also the public interest. Among other things, Defendants' failures have prevented government actors from investigating the Data Breach and preventing future harm, and they have eroded the public trust in companies like the Defendants who are expected to prevent data breaches and be forthcoming about them when they do occur. Thus, injunctive and equitable relief aiming to remedy these issues is in the public interest, and the balance of equities supports such relief.

VII. CLASS ACTION ALLEGATIONS

114. Plaintiffs bring this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "Class members."

115. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiffs propose the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

> **Nationwide Class**: All natural persons residing in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

116. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose the following state-by-state claims in the alternative to the nationwide claims, as well as statutory claims brought under state data breach and consumer protection statutes, on behalf of statewide subclasses for applicable States, (the "Statewide Subclasses"), subject to amendment as appropriate:

> **[State] Subclass**: All natural persons residing in [name of state or territory] whose Personally Identifiable Information was compromised as a result of the Data Breach.

117. Excluded from the Class and Subclasses are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and Defendants' affiliates, legal representatives, attorneys, successors, heirs, and assigns. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

118. **Numerosity under Federal Rule of Civil Procedure 23(a)(1).** The members of the Class (and Subclasses) are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of tens of thousands of

persons whose data was compromised in the Data Breach, who can be identified by reviewing the Private Information exfiltrated from Defendants' databases.

119. **Commonality under Federal Rule of Civil Procedure 23(a)(2).** There are questions of law and fact common to Plaintiffs and Class members, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and the Class members' Private Information;

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

c. Whether Defendants truthfully represented the nature of their security systems, including their vulnerability to hackers;

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

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

f. Whether Defendants owed a duty to Class members to safeguard their Private Information;

g. Whether Defendants breached their duty to Class members to safeguard their Private Information;

h. Whether cyberhackers obtained, sold, copied, stored or released Class members' Private Information;

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

j. Whether the Class members suffered legally cognizable damages as a result of Defendants' misconduct;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants' conduct was negligent per se; and

m. Whether the Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

120. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the Class members because Plaintiffs' Private Information, like that of every Class member, was compromised in the Data Breach.

121. **Adequacy of Representation under Federal Rule of Civil Procedure (a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of Class members, including those from states and jurisdictions where they may not reside, and they have no disabling conflicts of interest that would be averse to the other Members of the Class. Plaintiffs have retained Counsel that are competent and experienced in litigating complex consumer class action litigation and, in particular, privacy class action litigation. Plaintiffs intend to prosecute this action vigorously.

122. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** Defendants have engaged in a common course of conduct toward Plaintiffs and the Class members, in that all Plaintiffs' and the Class members' data at issue here was stored by Defendants and accessed during the Data Breach. The common issues arising from Defendants' conduct affecting Class members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

123. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** 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. Absent a class action, most Class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by 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 presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

124. **Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** Defendants have failed to take actions to safeguard Plaintiffs' and Class members' Private Information such that injunctive relief is appropriate and necessary. Defendants have acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

125. **Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4).** In the alternative, this litigation can be brought and maintained as a class action with respect to particular issues, such as Defendants' liability with respect to the foregoing causes of action.

VIII. CAUSES OF ACTION

126. Plaintiffs bring these causes of action on behalf of the Nationwide Class and Subclasses, as defined herein.

A. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1: NEGLIGENCE
On behalf of Plaintiffs and the Nationwide Class,
or alternatively, on behalf of Plaintiffs and the Subclasses

127. Plaintiffs repeat and reallege Paragraphs 1-125, as if fully alleged herein.

128. The Defendants required Plaintiffs, Class and Subclass members to submit non-public, personal information in order to secure loans, mortgages, open bank accounts, and engage other financial services.

129. In providing their Private Information, Plaintiffs, Class and Subclass members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by cybercriminals.

130. Defendants, as entities that collect sensitive, private data from consumers such as Plaintiffs, Class and Subclass members, and likewise store and maintain that data, have a duty arising independently from any contract to protect that information.

131. Specifically, Key, as a financial institution, had a duty to Plaintiffs, Class and Subclass members to securely maintain the Private Information collected as promised, warranted, and in a reasonable manner which would prevent cybercriminals from accessing and exfiltrating this information.

132. Further, Key had a duty to ensure that any third-party vendor to whom Key disclosed that sensitive Private Information would store and maintain that Private Information in a reasonable manner that would prevent cybercriminals from accessing and exfiltrating this Private Information.

133. OSC had a similar, independent duty to the Plaintiffs to maintain the Private Information collected as promised, warranted, and in a reasonable manner which would prevent cybercriminals from accessing and exfiltrating this Private Information.

134. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their systems and networks—and Plaintiffs, Class and Subclass members' Private Information held within their systems—to prevent disclosure of the information, and to safeguard the information from cyber theft.

135. Defendants' duty included a responsibility to implement systems and processes by which they could detect and prevent a breach of their security systems in an expeditious manner and to give prompt and adequate notice to those affected by a data breach and/or ransomware attack.

136. Defendants owed a duty of care to Plaintiffs, Class and Subclass members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected and safeguarded the Private Information of the Plaintiffs, Class and Subclasses.

137. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs, Class and Subclass members. While this special relationship exists independent from any contract, it is recognized by Keys' Privacy Policy, as well as applicable laws and regulations. Specifically, Defendants actively solicited Private Information as part of their business and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a resulting data breach.

138. Likewise, as the guardian and gatekeeper of Plaintiffs, Class and Subclass members' Private Information, a special duty existed between Defendants and Plaintiffs, Class and Subclass members to promptly and adequately provide notice of the Data Breach in a manner that would allow Plaintiffs, Class and Subclass members to take prompt and appropriate steps to safeguard their personal information.

139. Defendants also had a common law duty to prevent foreseeable harm to others. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

140. Defendants knew or should have known that the Plaintiffs, Class and Subclass members were relying on Defendants to adequately safeguard and maintain their Private Information.

141. Defendants had additional duties to safeguard Plaintiffs, Class and Subclass members' data through federal and state regulations, including the FTC Act and state consumer protection statutes.

142. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

143. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect the Plaintiffs, Class and Subclass members' data. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

n. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs, Class and Subclass members' Private Information;

o. Failing to adequately monitor the security of their networks and systems;

p. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

q. Allowing unauthorized access to and exfiltration of Plaintiffs, Class, Subclass members' Private Information; and

r. Failing to timely detect that Plaintiffs, Class and Subclass members' Private Information had been compromised.

s. .

144. It was foreseeable to Defendants that their failure to use reasonable measures to protect Plaintiffs, Class and Subclasses members' Private Information would result in injury to Plaintiffs, Class and Subclass members. Further, the breach of security was reasonably foreseeable given the known high frequency of cybersecurity attacks and data breaches.

145. It was therefore foreseeable to Defendants that their failure to adequately safeguard Plaintiffs, Class and Subclass members' Private Information would result in one or more types of injuries to Plaintiffs, Class and Subclasses members.

146. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

147. Plaintiffs are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate lifetime credit monitoring to all Class members, and any other relief this Court deems just and proper.

COUNT 2: DECLARATORY JUDGMENT
On behalf of Plaintiffs and the Nationwide Class,
or alternatively, on behalf of Plaintiffs and the Subclasses

148. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

149. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

150. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs, Class and Subclass members' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs, the Class and Subclass members from further, future data breaches that compromise their Private Information.

151. Plaintiffs, Class and Subclass members allege that Defendants' data security measures remain inadequate, and Defendants have not provided any evidence that they have

remedied the failure that occurred in the Data Breach at issue or have remedied any other vulnerability from their failure to properly assess threats by cybercriminals.

152. Plaintiffs, the Class and Subclass members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

153. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, the FTC Act and various state statutes;

b. Defendants owe a duty by virtue of their special relationship, understanding that they are safeguarding sensitive, Private Information, or that they have already acknowledged a responsibility to keep such information safe by virtue of security policies; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

154. If an injunction is not issued, Plaintiffs, the Class and Subclass members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants' systems. The risk of another such breach is real, immediate, and substantial. If another breach of Defendants' systems occurs, Plaintiffs, the Class and Subclass members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

155. The hardship to Plaintiffs, the Class and Subclass members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach of Defendants' systems occurs, Plaintiffs, the Class and Subclass members will likely be subjected to substantial identify theft and other damage (as they cannot elect to store their information with another company). On the other hand, the cost to Defendants

of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

156. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another data breach of Defendants' systems, thus eliminating the additional injuries that would result to Plaintiffs and the tens of thousands of consumers whose Private Information would be further compromised.

COUNT 3: INVASION OF PRIVACY
On behalf of Plaintiffs and the Nationwide Class,
or alternatively, on behalf of Plaintiffs and the Subclasses

157. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

158. Plaintiffs, Class and Subclass members have a legally protected privacy interest in their Private Information, which is and was collected, stored and maintained by Defendants, and they are entitled to the reasonable and adequate protection of their Private Information against foreseeable unauthorized access, as occurred with the Data Breach.

159. Plaintiffs, Class and Subclass members reasonably expected that Defendants would protect and secure their Private Information from unauthorized parties and that their Private Information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

160. Defendants unlawfully invaded the privacy rights of Plaintiffs, Class and Subclasses members by engaging in the conduct described above, including by failing to protect their Private Information by permitting unauthorized third parties to access, exfiltrate and view this Private Information.

161. This invasion of privacy resulted from Defendants' failure to properly secure and maintain Plaintiffs, the Class and Subclasses members' Private Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

162. Plaintiffs, the Class and Subclasses members' Private Information is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs, the Class and Subclasses members' Private Information, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

163. The disclosure of Plaintiffs, the Class and Subclasses members' Private Information to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

164. Defendants' willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and the Class and Subclasses members' sensitive, Private Information is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

165. The unauthorized access, exfiltration, and disclosure of Plaintiffs, the Class and Subclasses members' Private Information was without their consent, and in violation of various statutes, regulations and other laws.

166. As a result of the invasion of privacy caused by Defendants, Plaintiffs, the Class and Subclass members suffered and will continue to suffer damages and injury as set forth herein.

167. Plaintiffs, the Class and Subclasses members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

168. Plaintiffs and Class members are entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust

and adequate credit monitoring to Plaintiffs and Class and Subclass members; and any other relief this Court deems just and proper.

B. CLAIMS ON BEHALF OF THE STATE SUBCLASSES

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 4: INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code §§ 24-5-0.5-1, *et seq*.

169. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and alleges Paragraphs 1-125, as if fully alleged herein. This claim is brought individually under the laws of Indiana and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive consumer sales.

170. Defendants are a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

171. Defendants are a "supplier" as defined by § 24-5-0.5-2(a)(1), because they regularly engage in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

172. Defendants engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

173. Defendants' representations and omissions include both implicit and explicit representations.

174. Defendants' unfair, abusive, and deceptive acts, omissions, and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Indiana Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Indiana Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Indiana Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Indiana Subclass members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45 and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

175. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

176. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Indiana Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Indiana Subclass members into believing they did not need to take actions to secure their identities.

177. The injury to consumers from Defendants' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

178. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of their data security programs, Defendants created an asymmetry of information between them and consumers that precluded consumers from taking action to avoid or mitigate injury.

179. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

180. Defendants' acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Defendants' failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Defendants' data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and the Defendants concerning the state of Defendants' security.

d. Because Defendants took unreasonable advantage of consumers' reasonable reliance that they were acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

181. Defendants also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

182. Defendants intended to mislead Plaintiffs and Indiana Subclass members and induce them to rely on their misrepresentations and omissions.

183. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

184. Had Defendants disclosed to Plaintiffs and Class members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants were trusted with sensitive and valuable Private Information regarding tens of thousands of consumers, including Plaintiffs, the Class, and the Indiana Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of their security controls, and the security controls of their agents and representatives, secret from the public. Accordingly, because Defendants held themselves out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Indiana Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

185. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the Private Information in their possession. This duty arose because Defendants were trusted with sensitive and valuable Private Information regarding tens of thousands of consumers, including Plaintiffs, the Class, and the Indiana Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls, and the security controls of their agents and representatives, a secret from the public. Accordingly, because Defendants held themselves out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Indiana Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiffs and the Indiana Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in their systems;

b. Active concealment of the state of their cybersecurity; and/or

c. Incomplete representations about the security and integrity of their computer and data systems, and their prior data breaches, while purposefully withholding material facts from Plaintiffs and the Indiana Subclass that contradicted these representations.

186. Defendants acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiffs' and Indiana Subclass

members' rights. Defendants' actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

187. Plaintiffs will send a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 upon the filing of this Complaint, and will withdraw such cause of action if Defendants cure their unfair, abusive, and deceptive acts and practices within thirty (30) days. However, if such unfair, abusive, and deceptive acts and practices are not cured, or its violations of Indiana Deceptive Consumer Sales Act are incurable, Plaintiffs' cause of action will be perfected.

188. Since Plaintiffs provided the requisite notice, Defendants have failed to cure their violations of the Indiana Deceptive Consumer Sales Act.

189. Defendants' conduct includes incurable deceptive acts that Defendants engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

190. As a direct and proximate result of Defendants' uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiffs and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

191. Defendants' violations present a continuing risk to Plaintiffs and Indiana Subclass members as well as to the general public.

192. Plaintiffs and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the

greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 5: NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq*.

193. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-125, as if fully alleged herein. This claim is brought individually under the laws of New York and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive acts or practices.

194. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and New York Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

195. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

196. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the New York Subclass members, that their Private Information was not exposed and misled Plaintiffs and the New York Subclass members into believing they did not need to take actions to secure their personal information.

197. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights.

198. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

199. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the tens of thousands of New Yorkers affected by the Data Breach.

200. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

201. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

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

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class and Subclass members' Private Information, and to mitigate further harm;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity all types and kinds of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

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

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

G. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

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

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

X. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 19th day of October, 2022

Respectfully submitted,

/s/ *Mark Abramowitz*
MARK ABRAMOWITZ
mabramowitz@dicellolevitt.com
DICELLO LEVITT LLC
Western Reserve Law Building
7556 Mentor Ave
Mentor, Ohio 44060
Telephone: (440) 953-8888

AMY E. KELLER*
akeller@dicellolevitt.com
JAMES A. ULWICK*
julwick@dicellolevitt.com
DICELLO LEVITT LLC
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900

JAMES J. PIZZIRUSSO*
jpizzirusso@hausfeld.com
HAUSFELD LLP
888 16th Street, NW, Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200

STEVEN M. NATHAN*
snathan@hausfeld.com
KATHERINE HANSSON*
khansson@hausfeld.com
HAUSFELD LLP
33 Whitehall St., 14th Floor
New York, New York 10004
Telephone: (646) 357-1100

JEFFREY KALEIL*
jkaliel@kalielpllc.com
KALIEL GOLD PLC

1100 15th Street NW, 4th Floor
Washington, DC 20005
Telephone: (202) 350-4783

Counsel for Plaintiffs and the Proposed Class

**Pro Hac Vice Admission*
Applications Forthcoming

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MICHAEL J. BROUTY, MELISSA D. KAUFFMAN, and LEBERTUS VANDERWERFF

(b) County of Residence of First Listed Plaintiff New York
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Mark Abramowitz
DICELLO LEVITT LLC
Western Reserve Law Building

DEFENDANTS

KEYBANK NATIONAL ASSOCIATION, KEYCORP, and OVERBY-SEAWELL COMPANY

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)(A)

Brief description of cause:
Class action case against defendants responsible for a data breach.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ $5,000,001

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon. Charles Esque Fleming DOCKET NUMBER 1:22-cv-01536

DATE 10/19/2021

SIGNATURE OF ATTORNEY OF RECORD Mark Abramowitz

Digitally signed by Mark Abramowitz
Date: 2022.10.19 17:03:31 -05'00'

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

I. Civil Categories: (Please check one category only).

1. ☑ General Civil
2. ☐ Administrative Review/Social Security
3. ☐ Habeas Corpus Death Penalty

*If under Title 28, §2255, name the SENTENCING JUDGE: _____

CASE NUMBER: _____

II. **RELATED OR REFILED CASES** See LR 3.1 which provides in pertinent part: "If an action is filed or removed to this Court and assigned to a District Judge after which it is discontinued, dismissed or remanded to a State court, and subsequently refiled, it shall be assigned to the same Judge who received the initial case assignment without regardfor the place of holding court in which the case was refiled. Counsel or a party without counsel shall be responsible for bringing such cases to the attention of the Court by responding to the questions included on the Civil Cover Sheet."

This action: ☑ is **RELATED** to another **PENDING** civil case ☐ is a **REFILED** case ☐ was **PREVIOUSLY REMANDED**

If applicable, please indicate on page 1 in section VIII, the name of the Judge and case number.

III. In accordance with Local Civil Rule **3.8**, actions involving counties in the Eastern Division shall be filed at any of the divisional offices therein. Actions involving counties in the Western Division shall be filed at the Toledo office. For the purpose of determining the proper division, and for statistical reasons, the following information is requested.

ANSWER ONE PARAGRAPH ONLY. ANSWER PARAGRAPHS 1 THRU 3 IN ORDER. UPON FINDING WHICH PARAGRAPH APPLIES TO YOUR CASE, ANSWER IT AND STOP.

(1) **Resident defendant**. If the defendant resides in a county within this district, please set forth the name of such county

COUNTY: Cuyahoga

Corporation **For the purpose of answering the above, a corporation is deemed to be a resident of that county in which it has its principal place of business in that district.**

(2) **Non-Resident defendant.** If no defendant is a resident of a county in this district, please set forth the county wherein the cause of action arose or the event complained of occurred.

COUNTY:

(3) **Other Cases**. If no defendant is a resident of this district, or if the defendant is a corporation not having a principle place of business within the district, and the cause of action arose or the event complained of occurred outside this district, please set forth the county of the plaintiff's residence.

COUNTY:

IV. The Counties in the Northern District of Ohio are divided into divisions as shown below. After the county is determined in Section **III**, please check the appropriate division.

EASTERN DIVISION

☐	**AKRON**	**(Counties: Carroll, Holmes, Portage, Stark, Summit, Tuscarawas and Wayne)**
☑	**CLEVELAND**	**(Counties: Ashland, Ashtabula, Crawford, Cuyahoga, Geauga, Lake, Lorain, Medina and Richland)**
☐	**YOUNGSTOWN**	**(Counties: Columbiana, Mahoning and Trumbull)**

WESTERN DIVISION

☐	**TOLEDO**	**(Counties: Allen, Auglaize, Defiance, Erie, Fulton, Hancock, Hardin, Henry, Huron, Lucas, Marion, Mercer, Ottawa, Paulding, Putnam, Sandusky, Seneca VanWert, Williams, Wood and Wyandot)**

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.