UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MARC REICHBART, individually and on behalf of all others similarly situated, Plaintiff, v. FINANCIAL BUSINESS AND CONSUMER SOLUTIONS, INC., Defendant.	Case No. **COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiff Marc Reichbart ("Plaintiff"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, brings this class action against Defendant Financial Business and Consumer Solutions, Inc., ("FBCS" or "Defendant") and complains and alleges upon personal knowledge and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against FBCS for its failure to secure and safeguard his and approximately 1,955,385 other individuals' personally identifiable information, including names, Social Security numbers, dates of birth, and account information (collectively, "PII").

2. Defendant FBCS is a Pennsylvania-based debt collection agency that provides accounts receivable management and collection services across a variety of industries.[1]

3. FBCS reported that, on or about February 26, 2024, it "discovered unauthorized access to certain systems in its network" and subsequently "launched an investigation." FBCS's investigation revealed that its network "was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access." (the "Data Breach").[2]

4. FBCS provided limited details about the Data Breach, including whether or not the cybercriminal(s) responsible for breach were identified or whether the information exfiltrated was held for ransom. FBCS also did not disclose whether its investigation detected the compromised information on the dark web. Instead, FBCS stated that it "immediately took steps to conduct a diligent investigation to confirm the nature and scope of the incident" and "implemented additional safeguards in a newly built environment."[3] FBCS also offered access to credit monitoring and identity restoration services through CyEx at no charge to

[1] https://www.fbcs-inc.com/about-fbcs-collection-agency/ (last accessed May 2, 2024).
[2] Financial Business and Consumer Solutions, Inc., *Notice of Data Event*, OFFICE OF THE MAINE ATTORNEY GENERAL, available at https://apps.web.maine.gov/online/aeviewer/ME/40/5fe1ede5-aafd-4da2-b1a4-0057a6cdadc6.shtml (last accessed May 2, 2024).
[3] *Id.*

affected individuals but, as Plaintiff's allegations will make clear, this offer is woefully inadequate.

5. Despite learning of the Data Breach as early as February 26, 2024, FBCS did not announce the Data Breach publicly until April 26, 2024 and did not begin sending out Data Breach notification letters to affected individuals until around that time. According to FBCS's Notice, the information compromised in the Data Breach included names, Social Security numbers, dates of birth, and account information.[4]

6. FBCS's Notice did not disclose how it discovered the encrypted files on its computer systems were impacted, the means and mechanism of the cyberattack, the reason for the delay in notifying Plaintiff and the Class of the Data Breach, how FBCS determined that the PII had been "accessed or exfiltrated" during the Data Breach, and, importantly, what specific steps FBCS took following the Data Breach to secure its systems and prevent future cyberattacks.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII from the foreseeable threat of a cyberattack.

8. By being entrusted with Plaintiff's and Class Members' PII for its own pecuniary benefit, Defendant assumed a duty to Plaintiff and Class Members to

[4] *Notice of Data Event*, *supra* note 2.

implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' PII against unauthorized access and disclosure. Defendant also had a duty to adequately safeguard this PII under applicable law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"). Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in its possession from unauthorized access and disclosure.

9. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff and approximately 1,955,385 Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from the exposure, and the present and imminent thread of fraud and identity theft. This action seeks to remedy these failings and their consequences.

10. FBCS's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm.

11. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential PII remains in the

possession of Defendant. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

12. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to adequately train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members with prompt and adequate notice of the Data Breach.

13. In addition, Defendant failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

14. The security of Plaintiff's and Class Members' identities is now at risk because of Defendant's wrongful conduct, as the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

15. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in their names, using their

identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in Class Members' names, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. Moreover, because the exposed information includes Social Security numbers and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

18. Plaintiff and Class Members seek to hold Defendant responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of himself and all similarly situated individuals whose PII was accessed and exfiltrated during the Data Breach.

19. Plaintiff, individually and on behalf of all other Class Members, brings claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, breach of confidence, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiff and Class Members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to FBCS's data security protocols and employee training practices); reasonable attorneys' fees, costs, and expenses incurred in bringing this action; and all other remedies the Court deems just and proper.

PARTIES

Plaintiff

Plaintiff Marc Reichbart

20. Plaintiff Marc Reichbart is a resident and citizen of the state of Florida. Plaintiff provided his PII, or otherwise had his PII provided to, FBCS in connection with transacting with FBCS.

21. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years.

22. Plaintiff also suffered actual injury from having his PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and

diminution in the value of Plaintiff's confidential PII—a form of property that Plaintiff entrusted to FBCS, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff's privacy rights as a result of FBCS's unauthorized disclosure of PII.

23. As a result of FBCS's failure to adequately safeguard Plaintiff's information, Plaintiff has been injured. Plaintiff has experienced an uptick in spam calls and robocalls since shortly after the Data Breach. Plaintiff is also at a continued risk of harm because the PII remains in FBCS's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack so long as FBCS fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

Defendant

24. Defendant Financial Business and Consumer Solutions, Inc. is a Pennsylvania corporation with its principal place of business located at 330 S. Warminster Road, Suite 353, Hatboro, Pennsylvania 19040.

JURISDICTION AND VENUE

25. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there

are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

26. This Court has personal jurisdiction over FBCS because FBCS maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this District through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because FBCS resides in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

Overview of Financial Business and Consumer Solutions, Inc.

28. Founded in 1982, FBCS is nationally licensed debt collection agency that provides accounts receivable management and collection services across a variety of industries. FBCS is headquartered in Hatboro, Pennsylvania, with additional satellite offices in Cape May, New Jersey and Tampa, Florida[5], and boasts

[5] https://www.fbcs-inc.com/about-fbcs-collection-agency/ (last accessed May 2, 2024).

"more than 35 years of experience providing customer account management solutions for national creditors."[6]

29. In the regular course of its business, FBCS collects and maintains highly sensitive PII of consumers, clients, and employees. As a regular and necessary part of its business, FBCS collects and maintains highly sensitive PII from its clients, which is used to collect debts on behalf of its clients. That information includes, but is not limited to, names, Social Security numbers, dates of birth, and account information.[7] FBCS stores this information digitally.

30. FBCS is and was aware of the sensitive nature of the PII it collects, and it acknowledges the importance of data privacy. In its Privacy Policy on its website, FBCS claims that it "takes your privacy and security very seriously and has put significant privacy and security protections in place for our consumers, clients, and employees. These protections are designed utilizing industry privacy and security best practices to ensure your personal information is protected."[8]

31. In addition, the "Compliance & Technology" page on FBCS's website states:

> The security of our clients' data is our top priority at Financial Business and Consumer Solutions (FBCS). Our facilities and systems exceed the requirements for SSAE 18 Type II, PCI-DSS, and ISO 27001 certifications and we participate in regular audits to validate our policies, procedures and systems.

---

[6] *See* https://www.linkedin.com/company/fbcs-inc (last accessed May 2, 2024).
[7] *See Notice of Data Event*, *supra* note 2.
[8] https://www.fbcs-inc.com/privacy-policy/ (last accessed May 2, 2024).

> We operate on state of the art technology platforms that keep us compliant with information security requirements for large organizations and all state and federal regulations. Our advanced central administration system assists with the management of all our security policies and access privileges.
>
> The FBCS team is trained on security policies to keep our facilities and your data safe. We provide training to enhance our team's understanding of modern security risks, including social engineering attacks, phishing schemes, brute force attacks and more.[9]

32. By obtaining, collecting, using, and benefitting from Plaintiff's and Class Member's PII, Defendant assumed legal and equitable duties that required Defendant to, at a minimum, implement adequate safeguards to prevent unauthorized use or disclosure of PII and to report any unauthorized use or disclosure of PII.

The Data Breach

33. On or about February 26, 2024, FBCS "discovered unauthorized access to certain systems in its network" and subsequently "launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident."[10] FBCS's investigation revealed that its network "was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access."

[9] https://www.fbcs-inc.com/compliance/ (last accessed May 2, 2024).
[10] *Notice of Data Event*, *supra* note 2.

34. Despite learning of the Data Breach as early as February 26, 2024, FBCS did not announce the Data Breach publicly until April 26, 2024 and did not begin sending out Data Breach notification letters to affected individuals until around that time.

35. FBCS provided limited details about the Data Breach, including whether or not the cybercriminal(s) responsible for breach were identified or whether the information exfiltrated was held for ransom. FBCS also did not disclose whether its investigation detected the compromised information on the dark web. Instead, FBCS stated that it "immediately took steps to conduct a diligent investigation to confirm the nature and scope of the incident" and "implemented additional safeguards in a newly built environment." FBCS also offered access to credit monitoring and identity restoration services through CyEx at no charge to affected individuals.[11]

36. The Notice letters that FBCS sent to Plaintiff and the Class state that the information that was accessed included: names, Social Security numbers, dates of birth, and account information.[12]

37. FBCS's Notice omits pertinent information including how criminals gained access to the encrypted files on its systems, what computer systems were

[11] *Notice of Data Event, supra* note 2.
[12] *Id.*

impacted, the means and mechanisms of the cyberattack, the reason for the delay in notifying Plaintiff and Class Members of the Data Breach, how it determined that the PII had been accessed, and of particular importance to Plaintiff and Class Members, the actual steps FBCS took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

38. Based on FBCS's acknowledgment that "an unauthorized actor had the ability to view or acquire certain information on the FBCS network" during the Data Breach" and that "certain information … may have been accessed or exfiltrated during the incident," it is evident that unauthorized criminal actors did in fact access FBCS's network and exfiltrate Plaintiff's and Class Members' PII in an attack designed to acquire that sensitive, confidential, and valuable information.

39. The PII contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have accessed Plaintiff's and Class Members' PII.

40. The Data Breach reportedly impacted the PII of approximately 1,955,385 individuals.[13]

[13] *Id.*

FBCS Failed to Follow FTC Guidelines

41. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

42. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

43. According to the FTC, the need for data security should be factored into all business decision-making.

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.

45. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

46. 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.

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect 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. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Defendant failed to properly implement basic data security practices.

50. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

51. Defendant was at all times fully aware of its obligation to protect its customers' and employees' PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

FBCS Failed to Comply with Industry Standards for Data Security

52. Experts studying cybersecurity routinely identify corporations as being particularly vulnerable to cyberattacks because of the value of the PII that these entities collect and maintain.

53. Several best practices have been identified that at a minimum should be implemented by corporate entities like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, such as firewalls and anti-virus and anti-malware software; encryption (e.g., making data unreadable without a key); multi-factor authentication; backup data; and limiting the number of employees with access to sensitive data.

54. Other standard best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

55. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

56. These foregoing frameworks are existing and applicable industry standards in the corporate sector and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

FBCS Owed Plaintiff and Class Members a Duty to Safeguard Their PII

57. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

58. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

59. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner.

60. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

61. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

62. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of inadequate data security practices.

FBCS Knew That Criminals Target PII

63. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

64. At all relevant times, Defendant knew, or should have known, that Plaintiff's and all other Class Members' PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyberattacks that Defendant should have anticipated and guarded against.

65. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII

belonging to FBCS's consumers, clients, and employees, like Plaintiff and Class Members.

66. PII is a valuable property right.[14] The value of PII as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] Personal data is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

67. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various websites, making the information publicly available. This information from various breaches,

---

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[15] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, Medscape (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, p.4, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

68. Personally identifiable information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[22]

---

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

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

[20] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[21] *In the Dark*, VPNOverview.com, accessible at https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Jan. 25, 2024).

[22] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

69. Criminals can use stolen PII to extort a financial payment by "leveraging details specific to a disease or terminal illness."[23] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[24]

70. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[25]

71. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[23] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[24] *Id.*
[25] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

72. Indeed, cyberattacks have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[26]

73. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[27]

74. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated

[26] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.
[27] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

"[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[28]

Theft of PII has Grave and Lasting Consequences for Victims

75. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[29]

76. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[30] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number

[28] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[29] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on Jan. 25, 2024).

[30] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

to withdraw funds, obtain a new driver's license or other form of identification, and/or use the victim's information in the event of arrest or court action.[31]

77. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[32]

78. Each year, identity theft causes billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach

[31] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, Experian (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[32] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 2, 2024).

victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

79. Personally identifiable information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use the information and trade it on dark web black-markets for years to come.

80. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

81. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyberthieves get access to a person's highly sensitive information, they will use it.[33]

82. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial

[33] Ari Lazarus, *How fast will identity thieves use stolen info?*, Federal Trade Commission (May 24, 2017), available at https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[34]

83. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[35]

[34] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[35] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers,* Computer World (Feb. 6, 2015), https://www.redseal.net/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers/

85. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[36]

86. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of a Social Security number, and a new number will not be provided until after the victim has suffered the harm.

87. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[37]

88. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt

[36] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), accessible at https://www.idtheftcenter.org/identity-theft-aftermath-study/.
[37] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

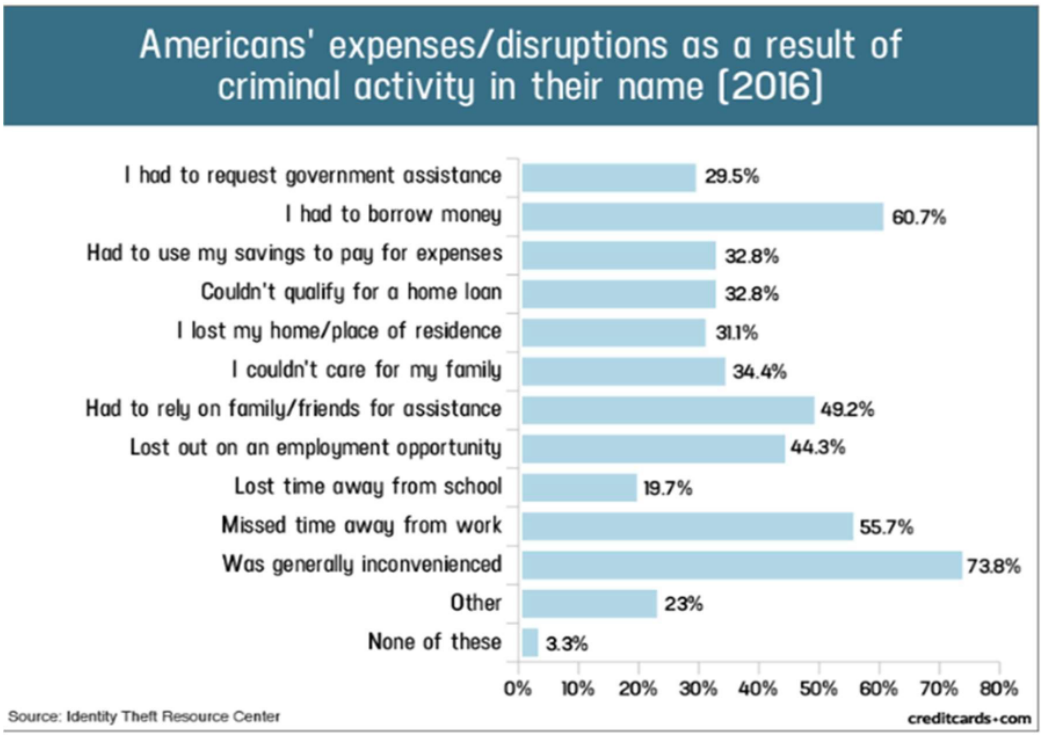
collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when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

89. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[38]

90. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

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

[38] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.



92. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[39]

93. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now m the time and expend the effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing

[39] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other account information for unauthorized activity for years to come.

94. Plaintiff and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including, but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

95. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown to be incapable of protecting Plaintiff's and Class Members' PII.

The Data Breach was Foreseeable and Preventable

96. Data disclosures and data breaches are preventable.[40] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all

[40] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).

cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[41] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[42]

97. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[43]

98. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[44]

99. Plaintiff and Class Members entrusted their PII to Defendant as a condition of receiving mortgage services. Plaintiff and Class Members understood and expected that Defendant or anyone in Defendant's position would safeguard their PII against cyberattacks, delete or destroy PII that Defendant was no longer

[41] *Id.* at 17.
[42] *Id.* at 28.
[43] *Id.*
[44] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed May 2, 2024).

required to maintain, and timely and accurately notify them if their PII was compromised.

Damages Sustained by Plaintiff and Class Members

100. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach. FBCS only offered single bureau "credit monitoring and identity restoration services … through CyEx"[45] but did not disclose how it determined eligibility. Not only did Defendant fail to provide adequate ongoing credit monitoring or identity protection services for individuals impacted by the Data Breach, but the credit monitoring identity theft protection services does nothing to compensate Plaintiff and Class Members for damages incurred, and time spent dealing with, the Data Breach.

101. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

102. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their

[45] *See Notice of Data Event*, *supra* note 2.

names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

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

104. Plaintiff and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

105. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

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

b. Purchasing credit monitoring and identity theft prevention;

c. Placing “freezes” and “alerts” with reporting agencies;

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

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

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

106. Plaintiff and Class Members suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their PII, a form of property that FBCS obtained from Plaintiff and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

107. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

108. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

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

110. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures, and protocols that were necessary to protect Plaintiff's and Class Members' PII.

111. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

112. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would result if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of the breach.

113. The risk of improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class Members' PII from that risk left the PII in a dangerous condition.

114. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

115. Plaintiff brings this class action individually and on behalf of all members of the following class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

> **Nationwide Class**
> All persons in the United States whose PII was compromised in the Data Breach disclosed by FBCS, including all persons who were sent notice of the Data Breach.

116. Alternatively, or in addition to the nationwide class, Plaintiff seeks to represent the following state class:

> **Florida Class**
> All persons in the state of Florida whose PII was compromised in the Data Breach disclosed by FBCS, including all persons who were sent notice of the Data Breach.

117. The nationwide class and the state class are collectively referred to as the "Class." Excluded from the Class are FBCS and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

118. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Plaintiff's claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

119. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, approximately 1,955,385 individuals' information was exposed in the Data Breach.

120. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether FBCS had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;

b. Whether they computer systems and data security practices employed by FBCS to protect Plaintiff's and Class Members' PII violated the FTC Act, and/or state laws and/or FBCS's other duties discussed herein;

c. Whether FBCS failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiff and Class Members suffered injury as a proximate result of FBCS's negligent actions or failures to act;

e. Whether FBCS failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII;

f. Whether an implied contract existed between Class Members and FBCS providing that FBCS would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members;

h. Whether FBCS's actions and inactions alleged herein constitute gross negligence;

i. Whether FBCS breached its duties to protect Plaintiff's and Class Members' PII; and

j. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

121. FBCS engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

122. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had PII compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by FBCS, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

123. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or in conflict with, the Class that Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

124. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against FBCS, so it would be impracticable for Class Members to individually seek redress from FBCS's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the Class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE

125. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

126. FBCS owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

127. FBCS knew, or should have known, the risks of collecting and storing Plaintiff's and Class Members' PII and the importance of maintaining secure systems. FBCS knew, or should have known, of the many data breaches that targeted companies holding significant amounts of PII in recent years.

128. Given the nature of FBCS's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, FBCS should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

129. FBCS breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII.

130. It was reasonably foreseeable to FBCS that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

131. But for FBCS's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

132. As a result of FBCS's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the

effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

133. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

134. FBCS's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as FBCS, of failing to employ reasonable measures to protect and secure PII.

135. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

136. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA intended to guard against.

137. It was reasonably foreseeable to FBCS that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release,

disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

138. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of FBCS's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

139. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

140. Plaintiff and Class Members either directly or indirectly gave FBCS their PII in confidence, believing that FBCS would protect that information. Plaintiff and Class Members would not have provided FBCS with this information had they known it would not be adequately protected. FBCS's acceptance and storage of

Plaintiff's and Class Members' PII created a fiduciary relationship between FBCS and Plaintiff and Class Members. In light of this relationship, FBCS must act primarily for the benefit of its clients, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

141. FBCS has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII of Plaintiff and Class Members it collected.

142. As a direct and proximate result of FBCS's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII, which remains in FBCS's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
BREACH OF IMPLIED CONTRACT

143. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

144. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for FBCS to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

145. Plaintiff and Class Members would not have provided their PII to Defendant, or would not have agreed to have that information provided to Defendant, had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

146. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

147. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

148. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

COUNT V
UNJUST ENRICHMENT

149. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

150. This claim is pleaded in the alternative pursuant to Fed. R. Civ. P. 8(d).

151. Plaintiff and Class Members conferred a monetary benefit upon FBCS in the form of monies paid for debt collection services or other services.

152. FBCS accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. FBCS also benefitted from the receipt of Plaintiff's and Class Members' PII.

153. As a result of FBCS's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

154. FBCS should not be permitted to retain the money belonging to Plaintiff and Class Members because FBCS failed to adequately implement the data privacy

and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

155. FBCS should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
BREACH OF CONFIDENCE

156. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

157. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed or provided to, collected by, and maintained by FBCS, and that was ultimately accessed or compromised in the Data Breach.

158. FBCS has a special relationship to its clients and other affiliated persons, such as Plaintiff and the Class Members.

159. Because of that special relationship, FBCS was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

160. Plaintiff and the Class directly or indirectly provided FBCS with their PII under both the express and/or implied agreement of FBCS to limit the use and disclosure of such information.

161. FBCS owed a duty to Plaintiff and the Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

162. FBCS had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII.

163. Plaintiff and the Class have a privacy interest in their personal matters, and FBCS had a duty not to disclose confidential information and records concerning its consumers, clients and employees.

164. As a result of the parties' relationship, FBCS had possession and knowledge of the confidential PII and confidential records of Plaintiff and the Class.

165. Plaintiff's and Class Members' PII is not generally known to the public and is confidential by nature.

166. Plaintiff and Class Members did not consent to nor authorize FBCS to release or disclose their PII to an unknown threat actor.

167. FBCS breached the duties of confidence it owed to Plaintiff and the Class when Plaintiff's and Class Members' PII was disclosed to unknown criminal hackers.

168. FBCS breached its duties of confidence by failing to safeguard PII, including by, among other things: (a) mismanaging its system and failing to identify

reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) designing and implementing inadequate cybersecurity safeguards and controls; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its consumers, clients and employees; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PII to a criminal third party.

169. But for FBCS's wrongful breach of its duty of confidences owed to Plaintiff and the Class Members, their privacy, confidences, and PII would not have been compromised.

170. As a direct and proximate result of FBCS's breach of confidences, Plaintiff and the Class have suffered and/or are at a substantial increased risk of suffering injuries, including:

a. The erosion of the essential and confidential relationship between FBCS and Plaintiff and the Class.

b. Loss of the privacy and confidential nature of their PII;

c. Theft of their PII;

d. Costs associated with the detection and prevention of identity theft;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

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

h. The imminent and certain impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to FBCS with the mutual understanding that FBCS would safeguard PII against theft and not allow access and misuse of their data by others;

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

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by FBCS; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PII.

171. Additionally, FBCS received payments for services with the understanding that FBCS would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' PII.

172. FBCS breached the confidence of Plaintiff and the Class Members when it made an unauthorized release and disclosure of their PII and, accordingly, it would be inequitable for FBCS to retain the benefit at Plaintiff's and Class Members' expense.

173. As a direct and proximate result of FBCS's breach of its duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF

174. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

175. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

176. Defendant owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' PII.

177. Defendant still possesses the PII of Plaintiff and Class Members.

178. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members.

179. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures

to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

180. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

181. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against FBCS as follows:

A. Certifying the Class as requested herein, designating Plaintiff as class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, individually and on behalf of the Class, seeks appropriate injunctive relief designed to prevent FBCS from experiencing another

data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft.

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 2, 2024

Respectfully submitted,

/s/ Andrew W. Ferich

Andrew W. Ferich (PA 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Melissa Clark (*pro hac vice* to be filed)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521

Telephone: (310) 474-9111
Facsimile: (310) 474-8585
mclark@ahdootwolfson.com

Counsel for Plaintiff and the Putative Class

ClassAction.org
