**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MASSACHUSETTS**

| | |
|---|---|
| IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION | MDL No. 1:23-md-03083-ADB<br><br>Judge Allison D. Burroughs |
| This Document Relates To:<br><br>JEFFREY SCOTT, BONNIE SCOTT, and PAUL F. BENDER, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>UNION BANK AND TRUST COMPANY and PROGRESS SOFTWARE CORPORATION,<br><br>Defendants. | Civil Action No. 1:23-cv-12436-ADB<br><br>**SECOND AMENDED CLASS ACTION COMPLAINT**<br><br>**JURY DEMAND**<br><br>[Leave to file granted on December 12, 2024] |

Plaintiffs Jeffrey Scott, Bonnie Scott, and Paul F. Bender, on behalf of themselves and all similarly situated persons, allege the following against Union Bank and Trust Company ("UBT") and Progress Software Corporation ("Progress Software") (collectively, "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

## I. INTRODUCTION

1. Plaintiffs incorporate the allegations contained in the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

2. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' names, addresses, dates

of birth, email addresses, and Social Security numbers (collectively, the "Private Information") from cybercriminal hackers.

3. Founded in 1917, UBT is a family-owned financial institution headquartered in Lincoln, Nebraska that provides banking services to its customers.

4. UBT utilized MOVEit Transfer software ("MOVEit"), provided by Progress Software, to store customer Private Information.

5. On or about May 31, 2023, Progress Software notified UBT that a zero-day vulnerability within MOVEit had allowed the Private Information of UBT's clients (the "Class Members") to be unlawfully accessed and compromised.

6. On or about June 30, 2023, UBT sent out data breach notice letters to individuals whose information was compromised as a result of the MOVEit vulnerability. The vulnerability allowed Cl0p, a well-known Russian cybergang, to gain access to UBT's MOVEit application on or around May 29, 2023 (the "Data Breach").

7. Plaintiffs and Class Members are now at an imminent and substantial risk of identity theft and various other forms of personal, social, and financial harm as a result of the Data Breach. This risk will remain for their respective lifetimes.

8. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. Now armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, obtaining government benefits, filing fraudulent tax returns, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

10. Therefore, Plaintiffs and Class Members have suffered, and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain with Defendant, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and their failure to prevent and timely detect the Data Breach.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. UBT owed a non-delegable duty to Plaintiffs and Class Members to implement and to maintain reasonable and adequate security measures to secure, protect and safeguard their Private Information against unauthorized access and disclosure including, but not limited to, ensuring that the third parties that it contracted with likewise implemented appropriate data security protection measures.

14. Upon information and belief, Defendants failed to properly implement adequate data security practices with regard to their computer networks, systems and applications that

housed the Private Information. Had Defendants properly monitored their networks, they would have discovered the Data Breach sooner.

15. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that Defendants collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendants' data security systems, and future annual audits.

17. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, invasion of privacy, and declaratory and injunctive relief.

## II. PARTIES

18. Plaintiff Jeffrey Scott is, and at all times mentioned herein was, a citizen of the State of Nebraska.

19. Plaintiff Bonnie Scott is, and at all times mentioned herein was, a citizen of the State of Nebraska.

20. Plaintiff Paul Bender is, and at all times mentioned herein was, a citizen of the State of Nebraska.

21. Defendant is a financial institution that maintains its headquarters in Lincoln, Nebraska.

22. Defendant Progress Software is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

23. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

24. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. Absent the Court's MDL Order No. 12 (Direct Filing Order), Plaintiffs could have directly filed their action in this District, as their claims arise out of—in part—the actions of Progress. Plaintiffs could have also filed their claims in the United States District Court for the District of Nebraska, as that Court has personal jurisdiction over Defendant UBT because UBT operates and is headquartered in Nebraska and conducts substantial business in that jurisdiction. Either jurisdiction would be appropriate, as substantial acts giving rise to this action have occurred in the respective jurisdictions such that the exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice.

26. Venue is proper in in this District because a substantial part of the events giving rise to this action occurred here.

## IV. FACTUAL ALLEGATIONS

### A. Defendants' Business and Collection of Plaintiffs' and Class Members' Private Information

27. UBT provides personal and business banking services, "[f]rom checking and savings to loans and wealth management."[1]

28. On its website, UBT states that, "Offering you exceptional service, along with protecting your privacy, is important to us."[2] In its Financial Privacy Notice (the "Privacy Policy"), UBT also touts its use of "security measures that comply with federal law" to protect its customers' information.

29. Additionally, UBT's Privacy Policy lists the limited business purposes for sharing the Private Information entrusted to it, including "[f]or [] everyday business purposes," "marketing purposes," "joint marketing with other financial companies," "affiliates' everyday business purposes," "[f]or [its] affiliates to market to you," and "[f]or nonaffiliates to market to you."[3]

30. As a prerequisite to receiving services from Defendants, Plaintiffs and Class Members entrusted Defendants with their Private Information and, in doing so, relied upon Defendants to keep their Private Information confidential from unauthorized disclosure.

31. Because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to their customers, Defendants' duties and obligations to Plaintiffs and Class Members included, but were not limited to, keeping their Private Information private; complying with industry standards related to data security and the maintenance of their customers' Private Information; informing their customers of their legal duties relating to data security and

[1] *See* https://www.ubt.com/personal (last visited on Sept. 7, 2023).
[2] *See* https://www.ubt.com/privacy (last visited on Sept. 7, 2023).
[3] *See* https://www.ubt.com/sites/default/files/files/2019-09/financial-privacy-bank-current.pdf (last visited on Sept. 7, 2023).

complying with all federal and state laws protecting customers' Private Information; only using and releasing customers' Private Information for reasons that relate to the services they provide; and providing timely and adequate notice to customers if their Private Information is disclosed without authorization.

32. UBT specifically understood the sensitive nature of Plaintiffs' and Class Members' Private Information. Being in the business of banking, UBT knows that the information it used Progress software to transfer and store Plaintiffs' and Class Members' data is the same information that is used to access accounts, open new accounts, and commit identity theft and fraud.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

34. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendants ultimately failed to do.

**B. The Data Breach**

35. According to Defendants' Notice sent to Plaintiffs and Class Members, unauthorized third parties accessed files that contained Plaintiffs' and Class Members' Private Information.

36. Defendants reported to the Maine Attorney General that the Data Breach occurred on or around May 29, 2023, but that they did not discover the Data Breach until June 9, 2023.[4]

[4] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/893229cd-b658-42aa-bb38-f976a32aae2f.shtml (last visited on Sept. 7, 2023).

37. According to Defendants, the Data Breach affected 204,291 UBT customers in total.

38. Defendants had obligations created by contract, industry standards, common law, federal and state law, and representations made to Plaintiffs and Class Members to use reasonable data security procedures and practices to keep their Private Information confidential and to protect it from unauthorized access and disclosure. Defendants failed in doing so.

39. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such Private Information confidential and secure from unauthorized access and to prevent (or at least timely detect) any security breaches.

40. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

41. Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

**C. Defendants Failed to Comply with FTC Guidelines**

42. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

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

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

44. The FTC further recommends that companies not maintain personally identifiable information ("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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

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

46. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and UBT specifically failed to verify that its third-party service provider was also implementing basic data security practices with respect to its secure file transfer application. Defendants' failures in this regard constitute unfair acts or practices prohibited by Section 5 of the FTCA.

47. Defendants were at all times fully aware of their obligation to protect the Private Information of their customers yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

**D. Defendants Failed to Comply with Industry Standards**

48. As noted above, experts studying cybersecurity routinely identify businesses, and especially financial institutions, as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

49. Some general industry best practices that should be implemented by businesses like Defendants include but are not limited to: educating all employees, using only strong password requirements, implementing multilayer security including firewalls, anti-virus and anti-malware software, using encryption, requiring multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

50. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiffs and Class Members.

51. Other best cybersecurity practices that are standard in the industry include: 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 protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

52. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

53. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

### E. UBT Failed to Comply with Federal Law Concerning the Protection of Financial Institution Customers' Personal Information

54. Section 501(b) of the Gramm-Leach-Bliley Act (the "GLBA") states in relevant part that bank regulators must establish regulations, which banks must comply with, that "insure the security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security or integrity of such records," and "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[5] The regulation's provisions became effective in July 2001 and have steered the discussion of customer information protection in banking ever since. Nevertheless, as the Data Breach demonstrates, Defendants failed to live up to these cybersecurity obligations.

55. The Federal Deposit Insurance Corporation ("FDIC") guidance to banks regarding unauthorized access to customer information defines "sensitive customer information" to mean "a customer's name, address or telephone number in conjunction with the customer's Social Security

[5] *See also* FDIC Financial Institution Letter FIL-68-2001 *available at* https://www.fdic.gov/news/inactive-financial-institution-letters/2001/fil0168a.html (last visited Sept. 7, 2023).

number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account."[6]

56. Here Defendants told the Maine Attorney General that the Data Breach concerned UBT customers' names, addresses, and Social Security numbers, among other data. As such, there is no question that the data involved here is what the FDIC would term sensitive customer information.

57. In addition, federal regulations require banks to closely oversee security of third-party vendors. Given the circumstances of the instant Data Breach it is apparent that UBT also failed to fulfill this requirement.

### F. Defendants Breached Their Duty to Safeguard Plaintiffs' and Class Members' Private Information

58. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for their staff, and ensuring that their (and their vendors' and suppliers') computer systems, networks, and protocols adequately protected the Private Information of Class Members.

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

[6] FIL-27-2005 (Sept. 7, 2005) *available at* https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html (last visited Sept. 7, 2023).

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

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect their customers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions and adequately supervise their vendors and/or suppliers;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above;

f. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

60. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted Private Information.

61. Had Defendants remedied the deficiencies in their information storage and security systems (and the maintenance and supervision thereof), followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

62. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted by Defendants' acts and omissions alleged herein. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to,

fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants and the value of their Private Information has diminished in light of its theft.

### G. Defendants Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

63. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[7] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

64. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

65. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more

[7] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Sept. 7, 2023).

information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

66. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

67. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' compromised Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

68. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[8] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[8] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Sept. 7, 2023).

69. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to 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 in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

70. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal informationin the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services,government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Securitynumber and it's not a good idea because it is connected to your life in so many ways.[9]

[Emphasis added.]

71. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

---

[9] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Aug. 28, 2023).

72. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[10] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

73. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that "*Fullz*" packages (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[12]

74. Likewise, the value of PII is increasingly evident in our digital economy. Many banking institutions, including Defendant, collect PII for purposes of data analytics and marketing. They collect it to better target customers and share it with affiliates and nonaffiliates for similar purposes.

---

[10] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Sept. 7, 2023).

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Sept. 7, 2023).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Sept. 7, 2023).

75. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[13]

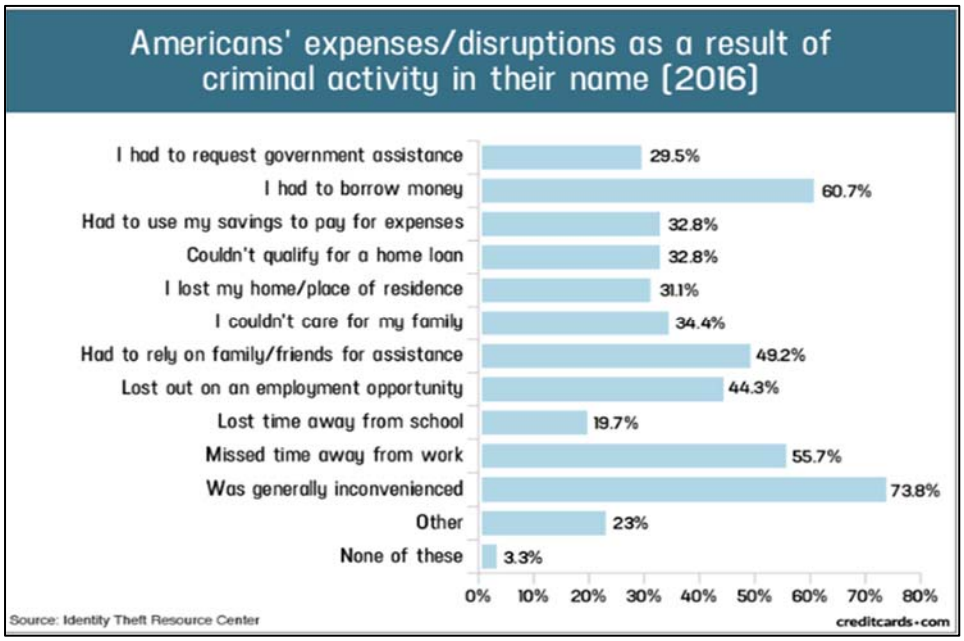
76. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it.

77. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

78. Data breaches, like that at issue here, cause real harm to consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

[13] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

79. A study by the Identity Theft Resource Center[14] shows the multitude of harms caused by fraudulent use of PII:




80. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[15]

> [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.

---

[14] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Sept. 7, 2023).

[15] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Sept. 7, 2023).

81. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.[16]

82. As a result, Plaintiffs and Class Members are at substantial increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts at a level of monitoring beyond that of an average person, with such monitoring to take place for many years.

## H. Plaintiffs' and Class Members' Damages

*The Scott Plaintiffs' Experience*

83. Plaintiff Jeffrey Scott and Plaintiff Bonnie Scott (the "Scott Plaintiffs") became customers of UBT in or around December of 2011.

84. When the Scott Plaintiffs first became customers and since, UBT requires them to provide it with substantial amounts of their PII.

85. Upon information and belief, UBT provided the Scott Plaintiffs' Private Information to Progress Software during the regular course of business.

86. On or about June 30, 2023, the Scott Plaintiffs received a letter entitled "Notice of Security Incident" which told them that their Private Information was accessed during the Data Breach. The notice letter informed them that the Private Information compromised included their "names, address, dates of birth, email addresses, and Social Security numbers."

87. The notice letter offered the Scott Plaintiffs only one (1) year of credit monitoring services. A single year of credit monitoring is not sufficient given that the Scott Plaintiffs will now

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737 (last visited Aug. 28, 2023).

experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of their Private Information.

88. The Scott Plaintiffs suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring their accounts for fraud.

89. The Scott Plaintiffs would not have provided their Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their customers' personal information from theft, and that those systems were subject to a data breach.

90. The Scott Plaintiffs suffered actual injury in the form of having their Private Information compromised as a result of the Data Breach.

91. The Scott Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their personal information – a form of intangible property that the Scott Plaintiffs entrusted to Defendants for the purpose of receiving banking and other financial services from Defendants and which was compromised in, and as a result of, the Data Breach.

92. The Scott Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being placed in the hands of criminals.

93. The Scott Plaintiffs have a continuing interest in ensuring that their Private Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

94. As a result of the Data Breach, the Scott Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach,

reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants, as well as long-term credit monitoring options they will now need to use. The Scott Plaintiffs have spent several hours dealing with the Data Breach, valuable time they otherwise would have spent on other activities.

95. As a result of the Data Breach, the Scott Plaintiffs have also suffered anxiety as a result of the release of their Private Information to cybercriminals, which Private Information they believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using their Private Information for purposes of committing cyber and other crimes against them. The Scott Plaintiffs are very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on their lives.

96. The Scott Plaintiffs also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of their Private Information, a form of property that Defendants obtained from the Scott Plaintiffs; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud they now face.

97. As a result of the Data Breach, the Scott Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

*Plaintiff Paul Bender's Experience*

98. Plaintiff Bender became a customer of UBT in or around 2009.

99. When Plaintiff Bender first became a customer, UBT required that he provide it with substantial amounts of his PII.

100. Upon information and belief, UBT provided Plaintiff Bender's Private Information to Progress Software during the regular course of business.

101. On or about June 30, 2023, Plaintiff Bender received a letter entitled "Notice of Security Incident" which told him that his Private Information had been subject to unauthorized access during the Data Breach. The notice letter informed him that the Private Information compromised included his "name, address, date of birth, and Social Security number."

102. The notice letter offered Plaintiff Bender only one (1) year of credit monitoring services. One (1) year of credit monitoring is not sufficient given that Plaintiff Bender will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

103. Plaintiff Bender suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

104. Plaintiff Bender would not have provided his Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their customers' personal information from theft, and that those systems were subject to a data breach.

105. Plaintiff Bender suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

106. Plaintiff Bender suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff Bender entrusted to Defendants for the purpose of receiving banking and other financial services from Defendants and which was compromised in, and as a result of, the Data Breach.

107. Plaintiff Bender suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

108. Plaintiff Bender has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

109. As a result of the Data Breach, Plaintiff Bender made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants, as well as long-term credit monitoring options he will now need to use. Plaintiff Bender has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

110. As a result of the Data Breach, Plaintiff Bender has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff Bender is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

111. Plaintiff Bender also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from Plaintiff Bender; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

112. As a result of the Data Breach, Plaintiff Bender anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

113. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

114. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

115. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

116. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

117. Further, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

118. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

119. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed

mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

120. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to UBT was intended to be used by UBT to fund adequate security of UBT's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

121. Additionally, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

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

123. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth

roughly $200 billion.[17] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[18]

124. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

125. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiffs and UBT included UBT's contractual obligation to provide adequate data security, which UBT failed to provide. Thus, Plaintiffs and Class Members did not get what they bargained for.

126. Finally, Plaintiffs and Class Members have suffered and/or will suffer actual injury as a direct and proximate result of the Data Breach 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. These losses may include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

---

[17] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion (last visited Sept. 7, 2023).

[18] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Sept. 7, 2023).

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

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

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

h. 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; and

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

127. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

128. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

## V. CLASS ACTION ALLEGATIONS

129. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

130. Specifically, Plaintiffs propose the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

131. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

132. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well to add subclasses, before the Court determines whether certification is appropriate.

133. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

134. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of over 204,000 customers whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through

Defendants' records, Class Members' records, publication notice, self-identification, and other means.

135. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. When Defendants learned of the Data Breach;

c. Whether Defendants' response to the Data Breach was adequate;

d. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. 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, including appropriate monitoring and supervision procedures and practices;

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

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

h. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

i. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

n. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

o. Whether Defendants' conduct was negligent;

p. Whether Defendants' conduct was *per se* negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

136. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

137. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

138. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

139. Superiority. A class action is superior to other available methods 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. 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 likely find that the cost of litigating their individual claims 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, conducting 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.

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

141. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

## VI. CLAIMS FOR RELIEF

### COUNT I
### NEGLIGENCE
### (On Behalf of Plaintiffs and the Nationwide Class against all Defendants)

142. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

143. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

144. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendants were on notice because, on information and belief, they knew or should have known that they would be an attractive target for cyberattacks.

145. Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect their customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA and GLBA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

146. Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

147. Defendants' duty also arose because Defendants were bound by industry standards to protect their customers' confidential Private Information.

148. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

149. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendants' possession.

150. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

151. Defendants, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

152. Defendants breached their duties, and thus weas negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks, systems and applications (and/or those of their vendors and/or suppliers);

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to comply with the FTCA and GLBA; and

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

153. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to adequately monitor, supervise, and protect their networks, systems and applications (and the Private Information that Defendants stored on them) from attack.

154. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

155. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

156. As a result of Defendants' negligence in breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

157. Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

158. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

159. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

160. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Defendants.

161. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

162. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, to strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

**COUNT II**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiffs and the Nationwide Class against all Defendants)**

163. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

164. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

165. Defendants breached their duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

166. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

167. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, and the industry-standard cybersecurity measures also set forth herein, form part of the basis of Defendants' duty in this regard.

168. Defendants violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

169. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

170. Defendants' violations of the FTCA constitute negligence *per se*.

171. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Defendants' negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

172. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the actual misuse of their Private Information and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

173. Defendants breached their duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

174. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

175. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

**COUNT III**
**BREACH OF CONTRACT**
**(On behalf of Plaintiffs and the Nationwide Class against Defendant UBT)**

176. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

177. Plaintiffs and Class Members entered into a valid and enforceable contract through which they entrusted their Private Information to UBT in exchange for services. That contract included promises by UBT, including those made in its Privacy Policy, to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

178. UBT's Privacy Policy memorialized the rights and obligations of UBT and its customers. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

179. In the Privacy Policy, UBT commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited business circumstances.

180. Plaintiffs and Class Members fully performed their obligations under their contracts with UBT.

181. However, UBT did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information from unauthorized disclosure, as promised in the Privacy Policy, and therefore UBT breached its contract with Plaintiffs and Class Members.

182. UBT allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, UBT breached the Privacy Policy with Plaintiffs and Class Members.

183. UBT's failure to satisfy its confidentiality and privacy obligations resulted in UBT's providing services to Plaintiffs and Class Members that were of a diminished value.

184. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in UBT's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

185. As a direct and proximate result of UBT's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

186. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring UBT to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

## COUNT IV
## BREACH OF IMPLIED CONTRACT
## (On Behalf of Plaintiffs and the Nationwide Class against UBT)

187. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

188. This Count is pleaded in the alternative to Count III above.

189. In connection with the dealings Plaintiffs and Class members had with Defendant, Plaintiffs and Class members entered into implied contracts with UBT.

190. Pursuant to these implied contracts, UBT agreed to provide services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with UBT regarding

the provision of those services through their collective conduct, including by Plaintiffs and Class Members giving their Private Information to UBT.

191. Through UBT's provision of services to Plaintiffs and Class Members, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its own policies, practices, and applicable law.

192. As consideration, Plaintiffs and Class Members turned over valuable Private Information to UBT. Accordingly, Plaintiffs and Class Members bargained with UBT to securely maintain and store their Private Information.

193. UBT accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members and using such Private Information for business purposes.

194. In delivering their Private Information to UBT, Plaintiffs and Class Members intended and understood that UBT would adequately safeguard the Private Information as part of that service.

195. UBT's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information, including its vendors, also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees and vendors is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or vendors; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

196. Plaintiffs and Class Members would not have entrusted their Private Information to UBT in the absence of such an implied contract.

197. Had UBT disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure their sensitive data, Plaintiffs and Class Members would not have provided their Private Information to UBT and would have banked elsewhere.

198. UBT recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

199. UBT violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

200. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain.

201. Plaintiffs and Class Members have been damaged by UBT's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

## COUNT V
## UNJUST ENRICHMENT
**(On Behalf of Plaintiffs and the Nationwide Class against all Defendants)**

202. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

203. This Count is pleaded in the alternative to Counts III and IV above.

204. Plaintiffs and Class Members conferred a benefit on Defendants by turning over their Private Information to Defendants and, in some cases, by paying money, in exchange for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

205. Upon information and belief, the monies paid by Plaintiffs and the Class to UBT were used by UBT, in part, to pay for Progress Software's secure file transfer application where Plaintiffs' and Class Members' Private Information was stored.

206. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendants also benefitted from the receipt of Plaintiffs' and Class Members' Private Information, as this was used in providing banking, marketing, and other services.

207. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that they failed to provide.

208. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and or are at an impending and substantial risk of suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the

impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

209. Additionally, Plaintiffs 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, and those payments without reasonable data privacy and security practices and procedures that they received.

210. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

211. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

## COUNT VI
## INVASION OF PRIVACY
**(On Behalf of Plaintiffs and the Nationwide Class against all Defendants)**

212. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

213. Plaintiffs and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendants, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the Data Breach. The PII of Plaintiffs and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

214. Plaintiffs and Class Members reasonably expected that Defendants would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

215. Defendants intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party.

216. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

a. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

b. failing to adequately secure their PII from disclosure to unauthorized persons; and

c. enabling the disclosure of their PII without consent.

217. This invasion of privacy resulted from Defendants' intentional failure to properly secure and maintain Plaintiffs' and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

218. Plaintiffs and Class Members' PII 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', and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

219. The disclosure of Plaintiffs' and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

220. Defendants' willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

221. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

222. As a direct and proximate result of Defendants' intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

## COUNT VII
## DECLARATORY JUDGMENT
**(On Behalf of Plaintiffs and the Nationwide Class against all Defendants)**

223. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

224. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state laws and regulations described in this Complaint.

225. Defendants owe a duty of care to Plaintiffs and Class Members, which required them to adequately secure Plaintiffs' and Class Members' Private Information.

226. Defendants still possess Private Information regarding Plaintiffs and Class Members.

227. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

228. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure their customers' Private Information and to timely detect and notify customers of a data breach under the common law, the GLBA, and/or Section 5 of the FTCA;

b. Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

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

229. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

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

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating their customers about the threats they face with regard to the security of their Private Information, as well as the steps Defendants' customers should continue to take to protect themselves.

230. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach within Defendants' systems and networks. The risk of another such breach is real, immediate, and substantial. If another breach occurs,

Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

231. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

232. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach within Defendants' networks and systems, thus preventing future injury to Plaintiffs and other customers whose Private Information would be further compromised.

## VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

## VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: July 3, 2024

Respectfully Submitted,

*/s/ Kristen A. Johnson*

Kristen A. Johnson (BBO# 667261)
**HAGENS BERMAN SOBOL SHAPIRO LLP**
1 Faneuil Hall Square, 5th Floor
Boston, MA 02109
Tel: (617) 482-3700
*kristenj@hbsslaw.com*

*Plaintiff's Liaison & Coordinating Counsel*

E. Michelle Drake
**BERGER MONTAGUE, PC**
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
*emdrake@bm.net*

Gary F. Lynch
**LYNCH CARPENTER, LLP**
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
*gary@lcllp.com*

Douglas J. McNamara
**COHEN MILSTEIN SELLERS & TOLL PLLC**
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
*dmcnamara@cohenmilstein.com*

Karen H. Riebel
**LOCKRIDGE GRINDAL NAUEN PLLP**
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
*khriebel@locklaw.com*

Charles E. Schaffer
**LEVIN SEDRAN & BERMAN LLP**
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
*cschaffer@lfsblaw.com*

*Plaintiff's Lead Counsel*

Mason A. Barney
Tyler Bean
**SIRI & GLIMSTAD LLP**
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Tyler W. Hudson
Eric D. Barton
**WAGSTAFF & CARTMELL, LLC**
4740 Grand Avenue, Suite 300
Kansas City, MO 64112
(816) 701-1100
thudson@wcllp.com

ebarton@wcllp.com

David S. Almeida
Elena Belov
**ALMEIDA LAW GROUP LLC**
849 W. Webster Avenue
Chicago, IL 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

*Counsel for Plaintiffs*

**CERTIFICATE OF SERVICE**

I hereby certify that, on this date, the foregoing document was filed electronically via the Court's CM/ECF system, which will send notice of the filing to all counsel of record.

Dated: December 16, 2024

*/s/ Kristen A. Johnson*

Kristen A. Johnson