UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

ANGIE BOUDREAUX and BARBARA WILLIAMS, on behalf of themselves and all others similarly situated, Plaintiffs, v. **SYSTEMS EAST, INC.,** a New York Domestic Business Corporation Defendant.	Lead Case No. 5:23-cv-01498-DNH-ML **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Angie Boudreaux and Barbara Williams ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Systems East, Inc. ("Systems East" or "Defendant") 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. Systems East is a software company that provides e-Payment solutions and online payment processing solutions through its cloud-based collections and digital bill payment products.[1] Systems East is also the parent company of a product called "Xpress Pay" through which it offers customers the ability to begin accepting electronic payments.[2]

[1] *See* https://www.systemseast.com/about/ (last visited January 23, 2024).
[2] *See* https://www.systemseast.com/solutions/electronic-payments/ (last visited January 23, 2024).

2. On November 16, 2023, Defendant notified its customers and various state Attorneys General about a widespread data breach that occurred on August 25, 2023.[3] Defendant did not discover this breach until October 27, 2023.[4]

3. On August 25, 2023, an unknown and unauthorized individual or individuals accessed Defendant's computer network and was able to steal an entire database that contained the names and payment card information of approximately 209,328 customers (the "Data Breach").[5] Indeed this criminal obtained everything they needed to illegally use Defendant's customers' credit cards to make fraudulent purchases, and to steal the customers' identities as shown by the numerous instances of fraud Plaintiff Boudreaux has already suffered as a direct result of the Data Breach.

4. Not only did the hacker(s) steal this personally identifiable information ("PII" or "Private Information"), but Plaintiff Boudreaux was also notified that her information was found on the Dark Web. Moreover, Plaintiff Boudreaux has also suffered numerous instances of fraud following the Data Breach and as a result of the Data Breach. This means that the Data Breach was successful, that the hacker(s) were able to access the unencrypted[6] information of both Plaintiffs and all "Class Members" (defined below), and that the hacker(s) were then able to offer for sale the unencrypted, unredacted stolen PII to criminals. Because of Defendant's breach,

[3] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/e73ef83d-a467-48f5-835f-167aac9bc315.shtml (last visited January 23, 2024).
[4] *Id.*
[5] *Id.*
[6] It is clear that the sensitive PII stolen in the Data Breach was not encrypted as shown by the fraud Plaintiff suffered as a direct result of the Data Breach, which would not be possible had the stolen PII and payment information actually been encrypted, and because Defendant disclosed the Data Breach and reported the Data Breach to the California Attorney General which is only required in the event of a data breach wherein unencrypted information was stolen. *See* Cal. Civ. Code § 1798.82.

customers' and website users' Private Information is still available on the Dark Web for criminals to access and abuse.

5. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to its failure to prevent the Breach, Defendant failed to detect it for more than two months.

6. Moreover, Defendant did not tell its customers or the Attorneys General about the Data Breach until almost another month after it was discovered.

7. Plaintiffs now bring this class action lawsuit to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' Private Information that it collected and maintained.

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

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

10. 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.

11. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

12. Plaintiff Angie Boudreaux, an individual, is, and at all times mentioned herein was, a citizen and resident of the State of Louisiana. Plaintiff Boudreaux utilized Defendant's e-Payment services through its "Xpress Pay" platform. She received Defendant's untitled notice of the Data Breach, dated November 16, 2023, on or about that date.

13. Plaintiff Barbara Williams, an individual, is, and at all times mentioned herein was, a citizen and resident of the State of South Carolina.

14. Defendant Systems East, a software solutions company, is a New York Domestic Business Corporation with its principal place of business located at 50 Clinton Ave, Cortland, New York 13045. At all times mentioned herein, Defendant operated in New York, Louisiana, and South Carolina through its website.

III. JURISDICTION AND VENUE

15. 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 Defendant. Indeed, both Plaintiffs Boudreaux and Williams are citizens of Louisiana and South Carolina, respectively, and Defendant Systems East is headquartered and incorporated in New York. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

16. This Court has personal jurisdiction over Defendant because Defendant operates in and is incorporated in New York and conducts business in the state.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in, were directed to, and/or emanated from this District.

IV. FACTUAL ALLEGATIONS

A. Defendant Systems East's Business and Collection of Plaintiffs' and Class Members' Private Information

18. Defendant Systems East is a cloud-based financial software company operating for more than 40 years. Defendant serves hundreds of thousands of customers in New York, South Carolina, Florida, and Arizona, among other states, by providing e-Payment solutions and online payment processing services.

19. As part of its business practices, Defendant requires the users of its software, such as Plaintiffs, to provide it with their Private Information, including but not limited to their names, addresses, email addresses, and payment card information, which includes all forms of PCI such as credit cards, debit cards, and more. On information and belief, Defendant also stores this sensitive information in its computer network for extended periods of time, as shown by the fact that hacker(s) were able to steal the sensitive Private Information of approximately 209,328 individuals in the Data Breach.

20. Defendant, by and through its Xpress-Pay website's Privacy Policy, promises that: "[i]f you do not explicitly instruct us to retain your credit/debit card information for future use, this payment information is erased immediately upon completion of the transaction[.]"[7] Defendant also states that it "respects [its customers'] privacy."[8] Moreover, Defendant represents that it "[p]rotects [customers' and website users'] information using the same enterprise level security as

[7] *See* https://info.xpress-pay.com/privacy-policy/ (last visited January 23, 2024).
[8] *Id.*

major banks."[9] Indeed, Defendant markets itself as a "secure and flexible e-Payment solution" on its website which is designed to entice its customers and users to trust that Defendant implements proper data security policies and procedures when it clearly does not.[10]

21. Defendant also promises via its Xpress-Pay website that:

> If, for your convenience, you elect to create an Xpress-pay Digital Wallet Account to expedite future payments, this information (excluding the CVV) is encrypted and stored in secure servers certified at Level One of the Payment Card Industry Data Security Standard (PCI DSS), the highest level of certification available. If you do not explicitly instruct us to retain your credit/debit card information for future use, this payment information is erased immediately upon completion of the transaction, whether or not the transaction is successful.[11]

22. Clearly, Defendant failed to implement the security features it promises its customers and e-Payment platform users that it will implement.

23. The PCI DSS (Payment Card Industry Data Security Standard) compliance sets forth numerous requirements for businesses that store, process, or transmit payment card data to observe. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that fail to maintain PCI DSS compliance are subject to steep fines and penalties.

24. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks, and using anti-virus software and updating it regularly.[12]

25. To make payments using Defendant's "Xpress-Pay" software/website, customers

---

[9] *See* https://www.systemseast.com/ (last visited January 23, 2024).
[10] *Id*.
[11] *See* https://info.xpress-pay.com/privacy-policy/ (last visited January 23, 2024).
[12] *See* PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last visited January 23, 2024).

and users can either create an account or check out as a guest. Either choice requires, at a minimum, that the customer enter the following PII onto the website:

- First and Last Name;
- Payee's Full Billing Address;
- Phone Number;
- Email;
- Credit/Debit Card Type;
- Full Credit/Debit Card Number;
- Credit/Debit Card Security Code or CSV Number; and
- Credit/Debit Card Expiration Date

26. Indeed, this sensitive PII and payment information is all that hackers would need to commit fraudulent and criminal acts against the individuals affected by the Data Breach.

27. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its users, it promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should

have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

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

B. The Data Breach and Systems East's Inadequate Notice to Plaintiffs and Class Members

30. On or about November 16, 2023, Defendant sent customers a seemingly innocuous, and untitled, Notice of Data Security Incident ("Notice").[13] In its untitled Notice, Defendant informed the recipients of the Notice that:

> **What Happened and What Information Was Involved?** On August 25, 2023, an unknown individual temporarily accessed certain systems on our computer network, which was identified and stopped the same day. In response, we undertook a review of what occurred and identified that an unknown individual copied an encrypted database file that contained your name and payment card information. We cannot confirm whether the unknown individual could decrypt that information. Please note, the database file did not contain additional information normally required to process a payment card transaction, including address or contact information, card verification value or security code, or magnetic stripe data.
>
> **What We Are Doing.** We notified the payment card providers (Visa, Mastercard, American Express, and Discover) about this matter so they could take steps to monitor your payment card information. We are also notifying you about this matter so you can take steps to monitor your payment card information. Additionally, we are evaluating our technical security measures and policies and have implemented enhancements to mitigate the risk of a matter like this reoccurring.
>
> **What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the "Steps You Can Take To Protect Personal Information" section of this letter to learn more about free resources that are available to assist you with protecting

[13] *See Supra*, at Footnote No. 3.

your information. [14]

31. On that same day, November 16, 2023, Defendant's Director of Operations, Peter Rogati, provided the same untitled Notice to the Attorneys General of the states where affected customers reside, including Maine[15] and California.[16]

32. Interestingly, the Notice sent to affected individuals and the Attorneys General states that law enforcement did not disclose that its customers' and website users' debit and credit cards were being offered for sale on the Dark Web; nor did it notify affected individuals of the severity of the Data Breach. Indeed, the untitled Data Breach letter does the complete opposite and instead lulls the affected individuals into a false sense of security by proclaiming that the stolen data was encrypted, that they "cannot confirm whether the unknown individual could decrypt [the stolen] information," and that affected individuals need not do anything other than "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."[17]

33. To make matters even worse, Defendant has not offered any form of credit monitoring or identity theft protection to the affected individuals.[18]

34. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

---

[14] *Id*.
[15] *See Supra*, at Footnote No. 3.
[16] *See* https://oag.ca.gov/ecrime/databreach/reports/sb24-576609 (last visited January 23, 2024).
[17] *See Supra*, at Footnote No. 3.
[18] *Id*.

Defendant failed to uphold its obligations and to honor the representations it made to Plaintiffs and Class Members regarding keeping their Private Information safe.

35. As a result of Defendant's failure to uphold its obligations and representations to Plaintiffs and Class Members, Defendant's customers' and website users,' including Plaintiffs' and Class Members', information was for sale on the Dark Web and, on information and belief, is still for sale to criminals. This means that the breach was successful; unauthorized individuals accessed Defendant's customers' unencrypted, unredacted information, including but not limited to name, phone number, email address, shipping address, billing address, payment card number, security or CVV code, and expiration date, and possibly more, without alerting Defendant, then offered the stolen information for sale online where Plaintiffs received a Notice that her information was found on the Dark Web. There is no indication that Defendant's customers' and website users' PII was removed from the Dark Web, where it remains to this day.

36. Defendant failed to comply with these obligations, leading to the compromise and sale of Plaintiffs' and Class Members' Private Information on the Dark Web.

C. Defendant Systems East Failed to Comply with FTC Guidelines

37. 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).

38. 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.

39. 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.

40. 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.

41. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

42. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Securing PII and Preventing Breaches

43. In a debit or credit card purchase transaction on an e-Payment platform, card data must flow through multiple systems and parties to be processed. Specifically:

> "When you use your credit card to order the book on the vendor's web site, you'll be asked to enter your credit card information, including the expiration date, three-digital card verification value code and address.
>
> Once you hit the submit button, a payment gateway comes into play. Its main job is to approve or deny payment requests.
>
> The gateway transfers information between a website or smartphone and your credit card bank account.
>
> It validates the accuracy of the payment information and uses security protocols and encryptions to make sure the transactions remain safe.
>
> The payment gateway forwards your purchase request to your company's credit card company. This company, in turn, verifies whether there's enough money in your credit card account to pay for the book.
>
> If so, the gateway sends the payment to the vendor."[19]

44. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: when the consumer submits their personal information and payment card information to the e-Payment platform, and when the e-Payment platform forwards this information to the vendor. This risk is greatly increased when the e-Payment platform, like Defendant's, stores consumer's personal information and payment information on its computer systems.

[19] *See* "*Electronic Payment Systems: Everything You Need to Know*" (July 26, 2022) *available at* https://www.avidxchange.com/blog/electronic-payment-systems-faqs-everything-you-need-to-know/ (last visited January 23, 2024).

45. Encryption mitigates security weaknesses that exist when consumer data has been stored by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the Private Information and payment card data the moment it is submitted, hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal and payment information stored in the e-Payment platform's computers. Defendant failed to implement such a simple solution, which would have protected its customers' Private Information. Additionally, to make matters worse, Defendant stored the Private Information, including payment information, on its computer network further exposing its website users' PII and payment card information to the risk of being stolen.

46. The financial fraud and other injuries outlined herein suffered by Plaintiffs and other customers demonstrates that Defendant (a) chose not to invest in the technology to encrypt payment card data ("PCD") at point-of-sale and in storage on its computer systems to make its customers' data more secure; (b) failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or (c) failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

47. These failures demonstrate a clear breach of the Payment Card Industry Data Security Standards (PCI DSS), which are industry-wide standards for any organization that handles PCD.

E. Defendant Systems East Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

48. In addition to its obligations under federal and state laws and industry standards, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining,

retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

49. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer 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, PCI DSS-compliant data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

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

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

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

51. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field and that were PCI DSS-compliant, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

52. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted by the Data Breach. 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 Defendant.

F. Defendant Systems East Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

53. 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.[20] 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.

54. 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

[20] *See 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 January 23, 2024).

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.

55. 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 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.

56. 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.

57. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' 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.

58. One such example of this is the development of "Fullz" packages.

59. Cybercriminals can cross-reference two sources of the Private Information

compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

60. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

61. 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.[21] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[21] *See IdentityTheft.gov,* Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited January 23, 2024).

62. 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.

63. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[22] 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.

64. 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.[23] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" sold for $30 in 2017.[24]

65. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including Defendant, collect PII for purposes of data analytics and marketing. These

[22] *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-four-members-china-s-military#:~:text=I%20am%20here%20to%20announce,all%20American%20citizens%2C%20and%20also (last visited January 23, 2024).

[23] *See 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 January 23, 2024).

[24] *See 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 January 23, 2024).

companies, collect it to better target customers, and shares it with third parties for similar purposes.[25]

66. 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."[26]

67. 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 by the economic benefit consumers derive from being able to use it and control the use of it.

68. 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.

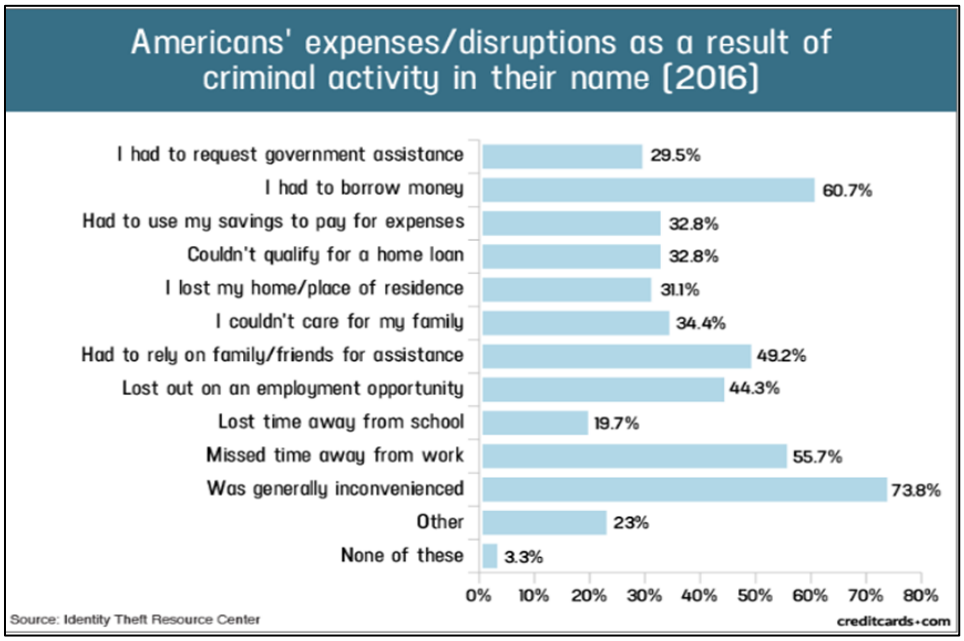
69. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

---

[25] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited January 23, 2024).

[26] *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).

70. A study by the Identity Theft Resource Center[27] shows the multitude of harms caused by fraudulent use of PII:



71. 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:[28]

> [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.

---

[27] *See* 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 January 23, 2024).

[28] *See 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/products/gao-07-737 (last visited January 23, 2024).

72. 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.

73. As a result, Plaintiffs and Class Members are at an 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 for many years to come.

G. Plaintiffs' and Class Members' Damages

Plaintiff Angie Boudreaux's Experience

74. Plaintiff Boudreaux was required to provide Defendant with her Private Information and PCD to access and utilize Defendant's Xpress Pay website.

75. Plaintiff Boudreaux suffered actual injury from having her Private Information and PCD compromised and/or stolen as a result of the Data Breach.

76. Plaintiff Boudreaux suffered actual injury and damages in paying money through and utilizing services from Defendant that she would not have utilized had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

77. Plaintiff Boudreaux suffered actual injury in the form of actual unreimbursed financial losses as a result of the fraud she suffered as a direct result of the Data Breach and damages to and diminution in the value of her personal and financial information – a form of intangible property that the Plaintiff Boudreaux entrusted to Defendant for the purpose of making payments through Defendant's website and which was compromised in, and as a result of, the Data Breach.

78. Plaintiff Boudreaux has also suffered numerous instances of fraud as a direct

result of the Data Breach. Specifically, after the Data Breach, Plaintiff Boudreaux suffered: (1) multiple fraudulent charges to her credit and debit cards and her bank account from multiple foreign companies, some of which were never reimbursed; (2) multiple fraudulent charges to her debit and credit card accounts for subscription services she never signed up for; (3) multiple notifications from her bank regarding an unauthorized third party making multiple duplicate charges to her bank account and purchasing cryptocurrency using her Coinbase account without her authorization; (4) an unauthorized third party opening an Uphold cryptocurrency account in her name and purchasing cryptocurrency multiple times using her debit and credit cards without her authorization; and (5) loss of access to her bank account, credit card account, and Coinbase account as a result of the numerous fraudulent charges to her accounts. On information and belief, Plaintiff Boudreaux believes that the unauthorized third party accessed her Coinbase account, and created an Uphold cryptocurrency account, utilizing the sensitive Private Information it acquired from the Data Breach, purchase cryptocurrency using her Private Information it acquired from the Data Breach, and then sent the purchased crypto currency to an anonymous cryptocurrency wallet; a transaction that is anonymous and largely untraceable. Indeed, this form of fraud has become more and more prevalent throughout the recent years and is the *modus operandi* of hackers who access, and sometimes purchase, victim's cryptocurrency accounts.[29]

79. Indeed, Plaintiff Boudreaux has suffered actual out-of-pocket and unreimbursed financial losses totaling more than $1,000.00 from the fraud she suffered as a direct result of the Data Breach.

80. Moreover, Plaintiff Boudreaux was notified by her Norton Antivirus software that

[29] *See* Justinas Baltrusaitis, "*Hacked Coinbase accounts on sale for as low as $610 on dark web*" (May 1, 2023) available at https://finbold.com/hacked-coinbase-accounts-on-sale-for-as-low-as-610-on-dark-web/ (last visited January 23, 2024).

her information was found on the Dark Web and has also been forced to purchase an application that screens the numerous scam and phishing calls she has been receiving on a daily basis.

81. Plaintiff Boudreaux suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

82. Plaintiff Boudreaux has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

83. As a result of the Data Breach, Plaintiff Boudreaux made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; dealing with the fraud she suffered as a direct result of the Data Breach; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Boudreaux has spent more than 40 hours dealing with the Data Breach, valuable time Plaintiff Boudreaux otherwise would have spent on other activities.

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

85. Plaintiff Boudreaux suffered actual injury from having her Private Information

compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Boudreaux; (b) violation of her privacy rights; (c) actual unreimbursed financial losses as a direct result of the Data Breach; (d) out-of-pocket expenses related to the purchasing of an application to screen the flood of scam and phishing calls she receives on an almost daily basis; and (e) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

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

Plaintiffs Barbara Williams' Experience

87. When Plaintiff Williams first became a user of Defendant's website, Defendant required her to provide it with substantial amounts of her PII, including her payment information. On or about November 16, 2023, Plaintiff received the Notice, which stated that her Private Information had been "copied" from Defendant's systems as a result of the Data Breach. The Notice further informed her that the Private Information compromised included her "name and payment card information."

88. The Notice declined to offer Plaintiff Williams any complimentary credit monitoring services.

89. Plaintiff has suffered actual injury in the form of time spent dealing with the Data Breach monitoring her accounts for fraud, given the increased risk of fraud resulting from the Data Breach.

90. Plaintiff would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its users' personal information from theft.

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

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

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

94. Plaintiff Williams has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

95. As a result of the Data Breach, Plaintiff 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 long-term credit monitoring options. Plaintiff has spent several hours dealing with the Data Breach – valuable time she otherwise would have spent on other activities.

96. As a result of the Data Breach, Plaintiff Williams has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of

committing cyber and other crimes against her. Plaintiff 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 her life.

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

98. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

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

100. As a direct and proximate result of Defendant's 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, fraudulent charges made on their financial accounts, credit card accounts opened in their names, and other forms of identity theft.

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

102. 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.

103. The Private Information maintained by and stolen from Defendant's 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.

104. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant. 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 Defendant was intended to be used by Defendant to fund adequate security of Defendant's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

105. Additionally, as a direct and proximate result of Defendant's 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.

106. 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.

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

was worth roughly $200 billion.[30] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[31]

108. 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.

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

110. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendant, 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.

---

[30] *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 January 23, 2024).

[31] *See Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited January 24, 2024).

111. As a direct and proximate result of Defendant's 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

112. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

113. Specifically, Plaintiffs propose the following Class, subject to amendment as appropriate:

> All individuals whose PII was accessed, acquired, and/or compromised as a result of the Data Breach announced by Systems East, Inc. on or about November 16, 2023 (the "Class").

114. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its 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.

115. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

116. 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 209,328 customers of Defendant whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

117. 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 Defendant engaged in the conduct alleged herein;

b. When Defendant learned of the Data Breach;

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

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

e. Whether Defendant 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;

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

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

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

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

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

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

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

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

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

o. Whether Defendant's conduct was negligent;

p. Whether Defendant's conduct was *per se* negligent;

q. Whether Defendant was unjustly enriched;

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

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

118. 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.

119. 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.

120. Predominance. Defendant has 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 Defendant's 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.

121. 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 Defendant. 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.

122. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2). Defendant has 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.

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

a. Whether Defendant owed a legal duty to Plaintiffs and Class members to exercise

due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

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

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

124. Finally, all members of the proposed Class are readily ascertainable. Defendant has 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 Defendant.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

125. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

126. Defendant 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.

127. Defendant 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. Defendant was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

128. Defendant owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Defendant's 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 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 its possession;

d. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the PCI DSS and consistent with industry-standard practices;

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

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

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

129. Defendant's 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.

130. Defendant's duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

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

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

133. Defendant, by its actions and/or omissions, breached its 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.

134. Defendant, by its actions and/or omissions, breached its 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.

135. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, its failure to:

a. Secure its e-commerce and e-Payment website;

b. Secure access to its servers and computer network;

c. Audit and monitor its severs and computer network;

d. Comply with industry standard security practices;

e. Follow the PCI-DSS standards;

f. Encrypt PCD at the point-of-sale, during transit, and at rest;

g. Employ adequate network segmentation;

h. Implement adequate system and event monitoring;

i. Utilize modern payment systems that provided more security against intrusion;

j. Install updates and patches in a timely manner; and

k. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

136. Defendant had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems (and the Private Information that it stored on them) from attack.

137. Defendant's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

138. Defendant's 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.

139. As a result of Defendant's negligence in breach of its 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.

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

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

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

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

144. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant 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 II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Class)

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

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

147. Defendant breached its duties by failing to employ industry-standard cybersecurity measures, including the PCI-DSS, in order to comply with the FTCA.

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

149. 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, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

150. 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 and industry standards would result in an unauthorized third-party gaining access to Defendant's networks, databases, and computers that stored Plaintiffs' and Class Members' Private Information.

151. Defendant's violations of the FTCA constitute negligence *per se*.

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

153. As a direct and proximate result of Defendant's 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 lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

154. Defendant breached its 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.

155. As a direct and proximate result of Defendant's 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.

156. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant 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 III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

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

158. When Plaintiffs and Class members provided their Private Information to Defendant in order to utilize the e-Payment services on its website, they entered into implied contracts under which Defendant agreed to protect their Private Information and timely notify them in the event of a data breach.

159. Defendant invited its customers and users, including Plaintiffs and the Class, to make payments to particular entities on its website using multiple different payment options, including but not limited to, debit and credit cards, in order to increase sales by making payments more convenient.

160. An implicit part of the offer was that Defendant would safeguard their Private Information using reasonable and industry-standard means and would timely notify Plaintiffs and Class Members in the event of a data breach.

161. Defendant also affirmatively represented in its Privacy Policy that it would protect the Private Information of Plaintiffs and Class members in several ways, as described above.

162. Based on the implicit understanding and also on Defendant's representations, Plaintiffs and Class Members accepted the offers and provided Defendant with their Private Information by using their payment cards in connection with e-Payments on the Defendant's website both before and during the period of the Data Breach.

163. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs' and Class Members' Private Information through, among other things, its Privacy Notice.

164. Defendant further demonstrated an intent to safeguard the Private Information of Plaintiffs and Class Members through its conduct. No reasonable person would provide sensitive, non-public information to any payment platform without the implicit understanding that the platform would maintain that information as confidential.

165. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

166. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information as promised or provide timely notice of a data breach.

167. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

168. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice when their Private Information was compromised in the Data Breach.

169. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breaches of its implied contracts with them.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

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

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

172. Plaintiffs and Class Members conferred a benefit on Defendant by turning over their Private Information to Defendant and by paying for products and services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

173. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including the revenue it generates as a result of the payments made by Plaintiffs and Class members.

174. As such, a portion of the payments made by Plaintiffs and Class Members while using Defendant's e-Payment services was to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry

standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

175. Defendant has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

176. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

177. If Plaintiffs and Class Members had known that Defendant had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

178. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant to be permitted to retain the benefit of its wrongful conduct.

179. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) 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; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) 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.

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

181. 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 V
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Class)

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

183. 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 statutes described in this Complaint.

184. Defendant owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

185. Defendant still possesses Private Information regarding Plaintiffs and Class Members.

186. Plaintiffs allege that Defendant's 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 her Private Information will occur in the future.

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

a. Defendant owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Defendant's existing security measures do not comply with its 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. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

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

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

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant 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 its 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 Defendant's 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 its users about the threats they face with regard to the security of their Private Information, as well as the steps Defendant's customers should take to protect themselves.

189. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

190. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant 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 Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

191. 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 at Defendant, 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 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 Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendant 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: January 26, 2024

Respectfully submitted,

/s/ Mason A. Barney

Mason A. Barney
NDNY Bar Roll No. 518229
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com

Rachele R. Byrd (*pro hac vice*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
E: byrd@whafh.com

Interim Co-Lead Class Counsel

M. Anderson Berry (*pro hac vice*)
Gregory Haroutunian
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Tel: 916.239.4778
Fax: 916.924.1829
E: aberry@justice4you.com
E: gharoutunian@justice4you.com

Additional Counsel for Plaintiffs and the Proposed Class

ClassAction.org
