

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

JOEL HOOD, ELIAS NEMIRI, GIDEON
BAUER, ELIZABETH GOLEC, and
ALEXYS TAYLOR, *individually and on
behalf of all others similarly situated,*

Plaintiffs,

v.

EDUCATIONAL COMPUTER SYSTEMS,
INC.,

Defendant.

This Document Relates to: All Actions

Master Docket No. 2:24-cv-00666-CCW

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Joel Hood, Elias Nemiri, Gideon Bauer, Elizabeth Golec, and Alexys Taylor (collectively “Plaintiffs”) by and through their undersigned counsel, file this Consolidated Amended Class Action Complaint individually and on behalf of a class of all similarly situated persons against Defendant Educational Computer Systems, Inc. (“ECSP” or “Defendant”). Plaintiffs allege as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge.

NATURE OF THE ACTION

1. The enormous amounts of valuable personally identifying information and financial information (collectively, “PII”) “that is shared online during tax season makes it a haven for thieves” as they do “everything they can to take full advantage of the opportunity tax season

brings.”¹ Despite cybercriminals’ yearly attempt to capitalize on the large amounts of PII shared online in preparation of each years’ April 15th tax deadline, ECSI, a sophisticated tax document services provider for colleges and universities across the country left its online services’ metaphorical back door unlocked, allowing cybercriminals to steal Plaintiffs’ and Class Members’ valuable tax documents. Even more bafflingly, ECSI failed to notice the theft for approximately four months.

2. ECSI provides financial management services to client colleges and universities (“University Clients”) including, *inter alia*, tax document services, past-due accounts receivable management, campus-based student loan servicing, tuition payment plans, refund management, and call center and outsourcing services.²

3. In order to provide services for its University Clients, ECSI collects, processes, and stores individuals’ PII such as names, Social Security numbers, addresses, and sensitive financial information, including information that can be found on tax forms such Form 1098-E and Form 1098-T. As ECSI is or should have been aware, these types of PII are highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, such sensitive data may be wielded to cause significant harm to Plaintiffs and the Class Members.

4. By collecting, storing, and processing PII that is highly sought after by cybercriminals, especially information that is routinely targeted during cybercriminals’ peak activity during the year, Defendant has a duty to secure, maintain, protect, and safeguard the PII with which it has been entrusted against unauthorized access and disclosure through reasonable

¹ <https://it.nc.gov/resources/online-safety-privacy/tips-guidance/avoiding-online-tax-scams> (last visited September 13, 2024).

² <https://home.ecsi.net/about-us> (last visited September 13, 2024).

and adequate data security measures. Indeed, ECSI expressly recognizes these duties, representing that it “take[s] the security and privacy of personal information seriously.”³

5. Despite ECSI’s duty to safeguard individuals’ PII, however, ECSI made the intentional choice to design its online services in such a way that students and borrowers could easily access and request their tax forms, including their Form 1098-Es and Form 1098-Ts via Defendant’s website without logging into their user profiles through a service called the “guest tax search functionality.”

6. Cybercriminals foreseeably took advantage of this design flaw in ECSI’s website, and exploited this vulnerability for approximately four months, with their malicious activity going unnoticed by Defendant from October 29, 2023 through February 12, 2024. By exploiting this vulnerability, the cybercriminals were able to gain access to Plaintiffs’ and Class Members’ PII contained on their Form 1098-Es and Form 1098-Ts (the “Data Breach”).⁴ This information included, *inter alia*, Plaintiffs’ names and Social Security numbers.⁵

7. As a direct and proximate result of Defendant’s failure to implement and follow basic security procedures, Plaintiffs’ and Class Members’ PII is now in the hands of cybercriminals.

8. Plaintiffs and Class Members have suffered identity theft, and are now at a significantly increased and certainly impending risk of continued fraud, identity theft, and other harms caused by ECSI’s failure to safeguard their PII—risks which will last for the rest of their

³ *Privacy Notice*, Educational Computer Systems, Inc. (Dec. 27, 2023), https://www.ecsi.net/privacy_notice.html.

⁴ *Notice of Data Breach*, Educational Computer Systems, Inc. (Apr. 2024), *template letter available at* <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/752b605d-f594-451a-a8f1-babb8cf37bbf.shtml> (last visited September 13, 2024).

⁵ *Id.*

lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. As such, on behalf of themselves and all others similarly situated, Plaintiffs bring claims for negligence, breach of implied contract, unjust enrichment, invasion of privacy, and declaratory judgment, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in ECSI's possession in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

10. Plaintiff Joel Hood is and, at all relevant times herein, was a resident and citizen of New York.

11. Plaintiff Elias Nemiri is and, at all relevant times herein, was a resident and citizen of Massachusetts.

12. Plaintiff Gideon Bauer is and, at all relevant times herein, was a resident and citizen of Virginia.

13. Plaintiff Elizabeth Golec is and, at all relevant times herein, was a resident and citizen of Rhode Island.

14. Plaintiff Alexys Taylor is and, at all relevant times herein, was a resident and citizen of Michigan.

15. Defendant ECSI is a Pennsylvania corporation that maintains its principal place of business at 1200 Cherrington Parkway, Suite 200, Coraopolis, PA 15108. Defendant ECSI is a citizen of the Commonwealth of Pennsylvania.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because Plaintiffs and at least one member of the Class, as defined

below, are citizens of a different state than Defendant, there are more than 100 members of each of the Class, and the aggregate amount in controversy exceeds \$5,000,000 exclusive of interests and costs.

17. This Court has general personal jurisdiction over Defendant because Defendant is a Pennsylvania corporation with a principal place of business located in Pennsylvania.

18. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(b)(1), because Defendant resides in this District, a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this District; Defendant conducts substantial business within this District; and Defendant has harmed Class Members residing in this District.

FACTUAL BACKGROUND

A. Defendant Provides Financial Management Services Involving Highly Sensitive Data.

19. ECSI "is the leading provider of past-due accounts receivable management, campus-based student loan servicing, tax document services, tuition payment plans, refund management, call center, and outsourcing services" providing its services to more than 1,750 University Clients nationwide.⁶

20. One of the services ECSI provides to University Clients is the "TaxSelect" service. In order to provide this service, ECSI collects and processes PII from its University Clients and generates tax forms, including Form 1098s for students and borrowers.⁷

21. A Form 1098-E is a Student Loan Interest Statement that reports the amount of money an individual paid in student loan interest that may entitle the individual to an income adjustment or a tax credit on their tax return.⁸ The information included on a Form 1098-E includes

⁶ <https://home.ecsi.net/about-us> (last visited September 13, 2024).

⁷ <https://home.ecsi.net/solutions/taxselect> (last visited September 13, 2024).

⁸ <https://studentaid.gov/articles/1098e-deduct-interest/> (last visited September 13, 2024).

the individual's student loan lender, the individual's Social Security Number or Tax Identification Number ("TIN"), their student loan account number, their mailing address, and the amount of loan interest paid.⁹

22. Similarly, a Form 1098-T is a Tuition Statement that reports tuition expenses an individual paid for college that may entitle the individual an income adjustment or tax credit on their tax return.¹⁰ The information included on a Form 1098-T includes similar information contained on a Form 1098-E, including the individual's Social Security Number or TIN, addresses, and total amounts paid by an individual for qualified tuition and related expenses.¹¹

23. In order to use this service to generate student and borrower Form 1098-Es and Form 1098-Ts, ESCI represents that its University Clients can simply submit a file to Defendant containing student and borrower PII. ESCI will then process this information to generate the required tax forms, deliver the tax forms to students and borrowers, and make the tax documents available to students and borrowers on ESCI's website.¹²

24. On information and belief, ESCI obtains students' and borrowers' Social Security numbers by requesting that each student and borrower complete and sign a W-9S form. Students and borrowers are obligated to complete and return W-9S forms when requested, or face a penalty of \$50. An entity that requests student and borrower information through a W-9S form, including the student's or borrower's SSN, is obligated to protect the SSN from unauthorized disclosure.

⁹ <https://www.irs.gov/pub/irs-pdf/f1098e.pdf> (last visited September 13, 2024).

¹⁰ <https://www.ed.gov/1098-e?src=rn> (last visited September 13, 2024).

¹¹ <https://www.irs.gov/pub/irs-pdf/f1098t.pdf> (last visited September 13, 2024).

¹² <https://go.ecsi.net/product-cutsheet-taxselect> (last visited September 13, 2024).

25. By providing a W-9S form to students and borrowers, ECSI promises the students and borrowers that it will protect the information provided on the form, including the individual's Social Security number or individual taxpayer identification number.

26. On information and belief, ECSI requires students and borrowers to create a profile with ECSI to obtain forms and access information concerning the individual's student loans. On ECSI's website, ECSI promises students and borrowers that it will protect their PI. Specifically, ECSI promises that it "take[s] the security and privacy of personal information seriously" and will maintain administrative, technical and physical safeguards designed to protect the personal information you provide against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use."¹³

27. In a second privacy policy, ECSI promises students and borrowers that ECSI will "protect your personal information from unauthorized access and use" by using security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."¹⁴

28. According to ECSI, over 1,000 University Clients use its TaxSelect service, and, through the TaxSelect Service, ECSI is involved in creating over six million tax documents annually.¹⁵

29. Upon information and belief, the PII ECSI collects, stores, and processes when providing its tax form services includes a wide variety of PII, including, *inter alia*, the names,

¹³ *Privacy Policy*, ECSI, https://www.ecsi.net/privacy_notice.html (last updated Dec. 27, 2023).

¹⁴ *Privacy Notice*, ECSI, https://www.ecsi.net/ECSI_GLBA_Privacy_Notice.html (last visited September 13, 2024).

¹⁵ <https://home.ecsi.net/solutions/taxselect> (last visited September 13, 2024).

Social Security numbers, TIN, and key financial information of its University Clients current and former students. This information is necessary to prepare the applicable tax documents.

30. As such, in order to obtain their tax documents from their respective colleges and universities, Plaintiffs and Class Members are required to either directly or indirectly entrust Defendant with their PII. In return, Plaintiffs and Class Members reasonably expected that ECSI would safeguard their highly sensitive information and keep it confidential.

31. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, ECSI assumed equitable and legal duties to safeguard and keep confidential Plaintiffs' and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

32. Defendant expressly recognizes its duty to safeguard Plaintiffs' and Class Members' PII, representing that "[w]e take the security and privacy of personal information seriously. We maintain administrative, technical and physical safeguards designed to protect the personal information you provide against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use."¹⁶

33. However, despite the existence of its duties and data security representations, ECSI failed to implement reasonable data security measures to protect the information with which it was entrusted, and ultimately allowed nefarious third-party hackers to compromise Plaintiffs' and Class Members' PII.

¹⁶ https://efpls.ed.gov/privacy_notice.html (last updated December 27, 2023).

B. The Data Breach.

34. Prior to February 12, 2024, ECSI's online services allowed students and borrowers to access their tax forms online, without requiring the user to log in to their accounts, by using Defendant's guest tax search functionality.¹⁷

35. Upon information and belief, Defendant's guest search tax function allowed students and borrowers to access their tax forms, including their Form 1098-Es and Form 1098-Ts by providing minimal information about themselves.

36. But the guest tax search functionality allowed more than just students and borrowers to access their tax forms. Without requiring any login or identity confirmation or data security measures, the guest tax search functionality allowed *anyone* (including cybercriminals with nefarious intentions) on the internet to access individuals' tax forms by supplying basic personal information that is available online and on the dark web.

37. Cybercriminals eventually discovered this critical vulnerability on ECSI's website and online services and exploited it for their own gain in a targeted attack designed to acquire Plaintiffs' and Class Members' PII.

38. Beginning on October 29, 2023, cybercriminals exploited the guest tax search functionality on Defendant's website and accessed Plaintiffs' and Class Members' PII housed within ECSI's online services, specifically information from Plaintiffs' and Class Members' Form 1098-Es and 1098-Ts.¹⁸

39. This unauthorized access to Plaintiffs' and Class Members' tax forms went unnoticed by ECSI for approximately four months. Indeed, Defendant inexplicably did not become aware of the unauthorized access until on or about February 12, 2024, when it noticed an

¹⁷ *Notice of Data Breach*, *supra* note 4.

¹⁸ *Id.*

“unusually high volume” of attempts to access its guest tax search functionality.¹⁹ It was only after detecting this unusually high volume of attempts to access the guest tax search function that spurred Defendant to take action to remedy the easily exploitable vulnerability, eventually shutting down the guest tax search functionality altogether.

40. Due to the vulnerabilities in the guest tax search functionality, these malicious third-party hackers gained access to and were able to acquire a wide array of PII contained on Plaintiffs’ and Class Members’ Form 1098-Es and 1098-Ts, including names, financial information (such as amount of tuition paid, scholarships received, or student loan interest paid), Social Security numbers, TINs, and other information contained on such forms.²⁰

41. More than two months after discovering the Data Breach and nearly six months after the Data Breach began, ECSI began notifying individuals impacted by the Data Breach on or about April 19, 2024.

42. Based on Defendant’s statements, cybercriminals intentionally accessed Defendant’s computer systems in an attack designed to access Plaintiffs’ and Class Members’ valuable PII stored therein, and these malicious hackers were successful in the attack.

43. As of today, more than eight months after the Data Breach commenced, ECSI still either does not know, or has not reported, the total number of individuals impacted by the Data Breach. However, due to the ordinary practice of ECSI’s business, it is evident that PII belonging to hundreds of thousands of students and borrowers, from ECSI’s 1,750 University Clients, were compromised in the Data Breach.

¹⁹ *Id.*

²⁰ *Id.*

44. By keeping affected individuals in the dark about the key details surrounding the Data Breach, ECSI prevented affected individuals from taking meaningful, proactive, and targeted mitigation measures that could help protect them against severe harm.

45. And when victims were eventually provided notice of the Data Breach, the notice letters acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

- a. “If you receive a letter from the IRS notifying you of a fraudulent return, please follow the instructions in that letter;”
- b. “Review the accompanying information on how to implement fraud alerts and credit freezes with credit agencies and obtain free credit monitoring services;”
- c. “We strongly recommend that all individuals take the following steps to help protect against data and identity theft: . . . Update passwords . . . Enable multi-factor authentication (MFA) on all accounts, where possible, Regularly check bank and credit card activity;”
- d. “remain vigilant against incidents of identity theft and fraud by reviewing your credit report/account statements for suspicious activity and to detect errors;”
- e. “enable fraud alerts;” and
- f. “place a credit freeze.”

46. Acknowledging that the victims of the Data Breach suffer impending risk of identity theft and misuse of their PII, Defendant offered complimentary credit monitoring in an attempt to mitigate such risk.

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

47. ECSI was well aware that the PII it acquired is highly sensitive and of significant value to those who would use it for wrongful and nefarious purposes.

48. ECSI also knew that a breach of its computer systems, and exposure and exfiltration of the PII stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised. Indeed, the data that ECSI collected, stored, and processed is a treasure trove for cybercriminals as this data contains all of the necessary information to commit identity theft and fraud.

49. These risks are not theoretical, numerous high-profile breaches have occurred at financial services companies in recent years, such as CapitalOne, KeyBank, Equifax, Flagstar Bank, and TMX Finance Corporate Services.

50. The ramifications of ECSI's failure to protect Plaintiffs' and the Class's PII is long lasting and severe, particularly given the risk of identity theft that Plaintiffs and the Class now face. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

51. The Federal Trade Commission ("FTC") recognizes identity theft as "a fraud committed or attempted using the identifying information of another person without authority."²¹ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

²¹ 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”²²

52. The Harvard Business Review notes, such “[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking.”²³

53. PII, including the information collected by ECSI, is highly valued by criminals, as evidenced by the prices that such information commands on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, a single victim’s personal information can be sold at prices ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁴ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²⁵

54. Moreover, there may be a time lag between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

²² *Id.*

²³ Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

²⁴ Anita George, *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs>.

²⁵ Brian Stack, *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web>.

As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁶

55. Data theft is not a hypothetical concern. In fact, the rate of cyberattacks has increased dramatically in recent years. In 2023, there were 3,205 publicly disclosed data compromises, affecting over 353 million victims. The U.S. specifically saw a 72% increase in data breaches from the previous all-time high in 2021 and a 78% increase over 2022.²⁷

56. Cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service issued a warning to potential targets to be aware of, and prepared for, a potential attack.²⁸

57. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, roughly 3.5 million people reported some form of identity theft, fraud, or other consumer complaint compared to 5.4 million people in 2023.²⁹

58. Moreover, the financial sector is a prime target for threat actors. Between January 2018 and September 2023, financial companies have suffered 2,260 data breaches, impacting over 232 million records.³⁰ The financial sector is “disproportionately targeted by threat actors” because

²⁶ Report to Congressional Requesters, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

²⁷ *2023 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

²⁸ FBI, *Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974>.

²⁹ *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Key%20Facts> (last visited September 13, 2024).

³⁰ Paul Bischoff, *Financial Data Breaches Accounted for 232 Million Leaked Records from January 2018 to September 2023*, Comparitech (Oct. 4, 2023), <https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/#:~:text=2%2C260%20financial%20data%20breaches%20from,over%20101%20million%20in%20total>.

of a simple rationale: “[t]hreat actors target organizations that have what they want and what pays big – data and money. Data can be sold for money and vulnerabilities that enable access to both data and money.”³¹

59. Companies that specifically target their financial services to clients in higher education are not immune to these attacks. In fact, in 2022, a student loan management technology service provider was targeted in a cyberattack impacting more than 2.5 million individuals.³²

60. Companies that provide tax document services are also frequently targeted by cybercriminals during tax season. “During tax season huge amounts of sensitive financial and identity data flows black and forth between individuals and organizations like the IRS and different kinds of tax services providers.”³³

61. Indeed, cybercriminals who steal taxpayer information have the data they need to commit tax and other crimes, and using this stolen information they commit a lot of it. For example, the IRS’s criminal investigation unit initiated more than 2,600 investigations that uncovered more than \$37 billion in tax and financial crimes in the fiscal year 2023.³⁴

62. The types of PII compromised in the Data Breach make the information particularly valuable to thieves and leaves the Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

³¹ Jen Miller-Osborn, *3 Reasons Cyberattacks Target Financial Services and How to Fight Back*, Paloalto Network (Aug. 31, 2021), <https://www.paloaltonetworks.com/blog/2021/08/financial-services-cyberattacks/>.

³² Bill Toulas, *Nelnet Servicing Breach Exposes Data of 2.5M Student Loan Accounts* (Aug. 29, 2022), <https://www.bleepingcomputer.com/news/security/nelnet-servicing-breach-exposes-data-of-25m-student-loan-accounts/>.

³³ <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/tax-season-cybersecurity-what-cybercriminals-want-and-who-they-target-most-is-it-you> (last visited September 13, 2024).

³⁴ <https://www.rightworks.com/blog/tax-season-security/> (last visited September 13, 2024).

63. Social Security numbers are particularly valuable since they allow individuals to file tax returns, apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often, Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

64. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person’s relationships with government agencies and any number of private companies in order to update the person’s accounts with those entities.

65. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new

number may make more difficult for you to get credit.³⁵

66. Moreover, even the theft of the last four digits of an individual's Social Security number can subject them to identity theft and fraud as companies and creditors often verify someone's identity by asking only for the last four digits, or the "serial number," of an individual's Social Security number. As such, cyber criminals armed with the last four digits of an individual's Social Security number, in combination with other personal information can open accounts, access an individual's name, or apply for benefits in that person's name.³⁶ Cybercriminals can also use computer programs to easily predict the first five digits of an individual's Social Security number, thus allowing them to determine an individual's full nine-digit number and commit even more types of fraud.³⁷

67. Even if cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of PII to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package that links that information together and sell the package at a higher price.

³⁵ *Identity Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

³⁶ Hari Ravichandran, *What Can Someone Do With Your Social Security Number*, Aura (Apr. 8, 2024), <https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number#:~:text=Many%20banks%2C%20government%20agencies%2C%20and,for%20benefits%20in%20your%20name.>

³⁷ Xenia Jardin, *Reverse-engineering SSNs from publicly available data*, BoingBoing (July 6, 2009), <https://boingboing.net/2009/07/06/reverse-engineering.html>.

69. Importantly, once a cybercriminal has a “Fullz” package, cybercriminals can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.³⁸ Most problematic, however, is that cybercriminals in possession of a “Fullz” package “are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures.”³⁹

70. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals 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.

71. The ramifications of ECSI’s failure to keep Plaintiffs’ and Class Members’ PII secure are thus long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

72. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

A direct financial loss is the monetary amount the offender obtained from misusing the victim’s account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not

³⁸ *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DataDome, <https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/#:~:text=Identity%20fraud%3A%20A%20set%20of,personal%20or%20business%2Drelated%20information> (last visited September 13, 2024).

³⁹ *Protection Against Fullz and Fraud, Integrity*, Aristotle (Apr. 18, 2022), <https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/>.

reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.⁴⁰

73. Due to high-profile data breaches at other companies, ECSI knew or should have known that its computer systems would be targeted by cybercriminals.

74. ECSI also knew or should have known the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were breached or if it otherwise failed to protect the PII in its possession. ECSI failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers PII from occurring.

D. Defendant Failed to Comply with FTC Guidelines and Industry Best Practices Regarding Data Security.

75. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by companies that handle or facilitate the handling of customer PII, including, but not limited to: establishing secure password and authentication procedures for employees; building secure networks by setting up network protection tools like firewalls and constantly monitoring for and patching vulnerabilities; encrypting sensitive data using robust encryption algorithms; limiting access to customer data to only relevant staff; and training staff regarding critical points.⁴¹

⁴⁰ Erika Harrell, *Bureau of Just. Stat.*, U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last visited August 2, 2024).

⁴¹ *Customer Data Security: Best Practices for Data Privacy*, CDP, <https://cdp.com/articles/customer-data-security-best-practices/> (last visited September 13, 2024); *Securing Networks: Best Practices for Cybersecurity in Telecommunications*, Prismecs, <https://prismecs.com/blog/securing-networks-best-practices-for-cybersecurity-in-telecommunications> (last visited September 13, 2024).

76. Government entities, including the FTC have similarly issued numerous guides for business outlining reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.⁴²

77. In *Start with Security: A Guide for Business*, for example, the FTC recommends that all companies:

- a. Identify all connections to the computers where sensitive information is stored;
- b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;
- d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;
- e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

⁴² *Start with Security: A Guide for Business* at 2, FTC (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

- f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;
- g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;
- h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and
- i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

78. The FTC further promulgated additional cybersecurity obligations for businesses in the later published *Protecting Personal Information: A Guide for Business*, which recommends the following best practices:⁴³

- a. Conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;
- b. Encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- c. Crafting a data security plan that involves both physical security (e.g., locking up physical files) and electronic security, and training employees regarding the data security plan;
- d. Promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and
- e. Developing a plan to handle a data breach or data security incident, if and when such an incident occurs.

79. The FTC further recommends that companies verify that any third-party service providers have implemented reasonable security measures.⁴⁴

⁴³ *Protecting Personal Information: A Guide for Business*, U.S. Federal Trade Comm’n (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited September 13, 2024).

⁴⁴ Erika Harrell, Bureau Just. Stat., U.S. Dep’t of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last visited September 13, 2024); <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited September 13, 2024).

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. Upon information and belief, Defendant failed to properly implement one or more of the basic data security practices described above. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized release of Plaintiffs' and Class Members' PII to threat actor. Further, Defendant's failure to implement basic data security practices constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

82. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.⁴⁵

83. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.⁴⁶ Upon information and belief, ECSI failed to adhere to the NIST guidance.

84. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the financial industry, including the following:

⁴⁵ See *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf> (last visited September 13, 2024).

⁴⁶ *Id.* at Table 2 pg. 26-43.

- a. Regularly assessing risks and auditing cybersecurity;
- b. Establishing a cybersecurity policy;
- c. Appointing a data protection officer;
- d. Securing networks;
- e. Verifying user identities;
- f. Establishing secure password management;
- g. Continuously monitor user activity; and
- h. Manage third-party risks.⁴⁷

85. Upon Information and belief, ECSI's failure to protect Plaintiffs' and Class Members' PII is a result of its failure to adopt reasonable safeguards as required by the FTC, NIST, and industry best practices.

86. ECSI was, at all times, fully aware of its obligation to protect the PII of its clients' students and borrowers because of its business model of collecting and storing PII. ECSI was also aware of the significant repercussions that would result—and have already resulted—from their failure to do so.

E. The Data Breach Put Plaintiffs and Class Members at Imminent and Substantial Risk of Fraud, Identity Theft, and Other Cybercrimes

87. ECSI's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, addresses, Social Security Numbers, and other financial information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and

⁴⁷ *12 Best Practices for Banking and Financial Cybersecurity Compliance*, Ekran (July 17, 2023), <https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance>.

substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

88. Plaintiffs' PII was stolen because it is highly valuable and useful to cybercriminals. Malicious actors can use stolen PII such as a victim's name, date of birth, and Social Security number to, among other things, gain access to consumers' bank accounts, social media, credit card accounts, and other consumer accounts. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain unemployment or other government benefits, obtain government IDs, or create "synthetic identities," whereby a cybercriminal combines real and fake information to create a new "synthetic" identity which makes it even easier to commit fraud.

89. Importantly, even if a full Social Security number is not compromised in a Data Breach, as noted previously, cybercriminals can easily use the information involved in the Data Breach to reverse engineer an individual victim's full Social Security number. Using nothing but an individual's date of birth and state of residence, computer programs can easily predict the first five digits of an individual's Social Security number.⁴⁸ Cybercriminals can combine these reverse-engineered digits with the last four digits stolen in the Data Breach, and then use the victim's full, nine-digit Social Security number to gain access to the victim's accounts and commit more complicated types of fraud.

90. Once cybercriminals start committing fraud and other identity theft-related crimes using a victim's PII, the disruption to the victim's life can be catastrophic. A study by the Identity Theft Resource Center ("ITRC") found that, among individuals who experienced fraudulent use

⁴⁸ Xenia Jardin, *Reverse-engineering SSNs from publicly available data*, BoingBoing (July 6, 2009), <https://boingboing.net/2009/07/06/reverse-engineering.html>.

of their PII, nearly all of them had experienced some form of costs or other harm in their lives, including having to borrow money, being forced out of their home or residence, and being unable to care for their family.⁴⁹ Indeed, as the U.S. Government Accountability Office (“GAO”) found in a 2007 report, victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”⁵⁰

91. Further, although the theft of PII creates an imminent risk of becoming a victim of identity theft and fraud, malicious actors often wait months or years to use the PII obtained in data breaches. The U.S. Government Accountability Office determined that “stolen data may be held for up to a year or more before being used to commit identity theft,” and that “once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.”⁵¹ During this delay, victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. Some of the Plaintiffs and many of the Class Members are in their twenties and thirties, and these Plaintiffs must vigilantly monitor their financial accounts for many, many years to come.

92. Cybercriminals will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiffs’ and Class Members’ data may have been compromised in other data breaches, the fact

⁴⁹ Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), <https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (captured on December 15, 2017).

⁵⁰ *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (“GAO Report”) at 2, U.S. Gov’t Accountability Office (June 2007), <https://www.gao.gov/assets/270/262899.pdf>.

⁵¹ U.S. Gov’t Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm>.

that the Data Breach centralizes the PII and identifies the victims as student loan borrowers materially increases the risk to Plaintiffs and the Class.

93. Even if cybercriminals use Plaintiffs' and Class Members' data to commit fraud and identity theft imminently, there is often a lag between when a person suffers harm due to theft of their PII and when they *discover* that harm. The substantial and imminent risk that Plaintiffs currently face therefore will not decrease over the next several months and years, and Plaintiffs will need to spend time and money to continuously monitor their accounts for years to ensure their PII is not used in malicious ways to harm them.

F. Plaintiffs and Class Members Suffered Damages.

94. The ramifications of ECSI's failure to keep consumers' PII secure are long-lasting and severe. ECSI's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways, including theft of their PII, identity theft and misuse of their PII, as well as substantial and imminent risk of ongoing or future identity theft and fraud. Plaintiffs and Class Members must immediately devote time, energy, and money to: (a) remediate the actual misuse of their PII; (b) closely monitor their bills, records, and credit and financial accounts; (c) change login and password information on any sensitive account even more frequently than they already do; (d) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (e) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

95. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.⁵² Its appendix of steps

⁵² Government Accountability Off., *Data Breaches* (Mar. 2019) <https://www.gao.gov/assets/gao-19-230.pdf>.

consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiffs and Class Members) must take after a data breach are both time-consuming and of only limited and short-term effectiveness.

96. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁵³

97. Further, once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or protected against future misuse.

98. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁵⁴

99. For these reasons, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of ECSI's conduct.

⁵³ See *Identity Theft Victim Checklist*, Fed. Trade Comm'n, <https://www.identitytheft.gov/Steps> (last visited September 13, 2024).

⁵⁴ See 2007 GAO Report, at 29.

100. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII 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.⁵⁵ In 2022, the data brokering industry was valued at more than \$268 billion.⁵⁶ In fact, the data marketplace is so sophisticated that consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$50 a year.⁵⁷

101. The value of Plaintiffs' and Class Members' PII has been diminished by its exposure in the Data Breach. Plaintiffs' and Class members' PII is a valuable commodity to identity thieves and, in all likelihood, is already being hotly traded on the dark web, or, at the very least, is already being used by identity thieves. And, once it has been compromised, criminals will use it and trade the information on the cyber black market for years thereafter.⁵⁸

102. The reality is that cybercriminals seek nefarious outcomes from a data breach, and stolen PII can be used to carry out a variety of crimes.

103. Plaintiffs and Class Members are also at a continued risk because their information remains in ECSI's systems, which have already been shown to be susceptible to compromise and

⁵⁵ See, e.g., Data Coup, <https://datacoup.com/> ("It's time to capture, control and profit from your personal data.") (last visited September 13, 2024).

⁵⁶ *Data Broker Market: Global Industry Analysis and Forecast (2023-2029)*, Maximize Market Research, <https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/> (last visited September 13, 2024).

⁵⁷ *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited September 13, 2024).

⁵⁸ *The Price Cybercriminals Charge for Stolen Data*, Trustwave (Aug. 6, 2023), <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/>.

attack and is subject to further attack so long as ECSI fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

104. As a result of ECSI's failures and the resulting Data Breach, Plaintiffs and Class Members have suffered from actual misuse of their PII, and further face an increased risk of identity theft and fraud, phishing attacks, and related cybercrimes. Those impacted are under heightened and prolonged anxiety and fear, as they have been or will be at risk of falling victim to cybercrimes for years to come.

105. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the actual misuse of their PII, increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers and cybercriminals.

106. Many victims of the Data Breach, including Plaintiffs, have already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including remediating actual misuse of their PII, obtaining credit monitoring services, reviewing financial statements, checking credit reports, and spending time and effort searching for unauthorized activity.

107. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;

- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.⁵⁹

108. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.⁶⁰

109. Plaintiffs and Class Members have a direct interest in ECSI's promises and duties to protect their PII, *i.e.*, that ECSI *not increase* their risk of identity theft and fraud. Because ECSI failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by ECSI's wrongful conduct. Through this remedy, Plaintiffs and Class Members seek to restore themselves and Class Members as close to the same position as they would have occupied but for ECSI's wrongful conduct, namely its failure to adequately protect Plaintiffs' and Class Members' PII.

⁵⁹ *Identity Theft: The Aftermath 2017*, ITRC, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited September 13, 2024).

⁶⁰ *Id.*

110. ECSI's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach. Furthermore, the Data Breach notice did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. ECSI's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach, ECSI prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

111. Because of ECSI's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, identity theft, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII is used;
- b. losing the value of the explicit and implicit promises of data security;
- c. the unconsented disclosure and publication of their PII;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identity theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII; and

- h. continued risk to their PII—which remains in Defendant’s possession—and is thus at risk for future breaches so long as Defendant fail to take appropriate measures to protect the PII.

112. Because ECSI continues to hold Plaintiffs’ and Class Members’ PII and financial account information, Plaintiffs and Class Members have an interest in ensuring that their PII and financial account information is secured and not subject to further theft.

G. Plaintiffs’ Experiences.

a. *Plaintiff Joel Hood*

113. Plaintiff Hood is a current student at Rensselaer Polytechnic Institute (“RPI”).

114. For purposes of receiving educational services from RPI, Plaintiff Hood was required to provide his highly sensitive information, including his PII and financial account information to RPI and/or Defendant.

115. On information and belief, RPI provided Plaintiff Hood’s PII and financial account information to Defendant in connection with the services RPI provides to Plaintiff Hood.

116. As a result of the Data Breach, Plaintiff Hood received a notice informing him that his PII had been accessed and obtained by unauthorized individuals in the Data Breach.

117. Plaintiff Hood takes care in protecting his PII from disclosure. Faced with the risk of the unauthorized disclosure of his PII, he is now forced to monitor his accounts for signs of fraud and identity theft and to devote valuable time and resources to the same.

118. Plaintiff Hood suffered emotional distress knowing that his highly personal information is no longer confidential and can be used for blackmail, extortion, identity theft, fraud, and any number of additional harms for the rest of his life.

119. As a direct and proximate result of the Data Breach, Plaintiff Hood suffered actual injury and damages from having his PII compromised including, but not limited to: (a) damage to

and diminution in the value of his PII; (b) loss of value, privacy, and confidentiality of his PII; (c) the cost of indefinite monitoring and protection of his financial accounts; (d) violation of his privacy rights; (e) loss of time; and (f) failure to receive the benefit of his bargain.

120. Plaintiff Hood has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

b. *Plaintiff Elias Nemiri*

121. Plaintiff Nemiri is a current student at RPI.

122. For purposes of receiving educational services from RPI, Plaintiff Nemiri was required to provide his highly sensitive information, including his PII and financial account information to RPI and/or Defendant.

123. On information and belief, RPI provided Plaintiff Nemiri's PII and financial account information to Defendant in connection with the services RPI provides to Plaintiff Nemiri.

124. Plaintiff Nemiri received a notice informing him that his PII had been accessed and obtained by unauthorized individuals in the Data Breach.

125. In mid-March 2024, Plaintiff Nemiri received notice informing him that an unauthorized tax return was filed in his name. Plaintiff Nemiri spent a significant amount of time investigating and attempting to resolve the fraudulent tax return issue.

126. Plaintiff Nemiri takes care in protecting his PII from disclosure. In light of the multiple prior instances of identity theft and the continued risk of the unauthorized use of his PII, he is now forced to monitor his accounts for signs of fraud and identity theft and to devote valuable time and resources to the same.

127. Plaintiff Nemiri suffered emotional distress knowing that his highly personal information is no longer confidential and can be used for blackmail, extortion, identity theft, fraud, and any number of additional harms for the rest of his life. He also experienced great stress upon learning of the fraudulent tax return.

128. As a direct and proximate result of the Data Breach, Plaintiff Nemiri suffered actual injury and damages from having his PII compromised including, but not limited to: (a) identify theft; (b) damage to and diminution in the value of his PII; (c) loss of value, privacy, and confidentiality of his PII; (d) the cost of indefinite monitoring and protection of his financial accounts; (e) violation of his privacy rights; (f) loss of time; and (g) failure to receive the benefit of his bargain.

129. Plaintiff Nemiri has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

c. *Plaintiff Gideon Bauer*

130. Plaintiff Bauer is a current student at RPI.

131. For purposes of receiving educational services from RPI, Plaintiff Bauer was required to provide his highly sensitive information, including his PII and financial account information to RPI and/or Defendant.

132. On information and belief, RPI provided Plaintiff Bauer's PII and financial account information to Defendant in connection with the services RPI provides to Plaintiff Bauer.

133. Plaintiff Bauer received a notice informing him that his PII had been accessed and obtained by unauthorized individuals in the Data Breach.

134. In early-March 2024, Plaintiff Bauer received notice informing him that an unauthorized tax return was filed in his name. Plaintiff Bauer spent a significant amount of time investigating and attempting to resolve the fraudulent tax return issue.

135. Plaintiff Bauer takes care in protecting his PII from disclosure. In light of the multiple prior instances of identity theft and the continued risk of the unauthorized use of his PII, he is now forced to monitor his accounts for signs of fraud and identity theft and to devote valuable time and resources to the same.

136. Plaintiff Bauer suffered emotional distress knowing that his highly personal information is no longer confidential and can be used for blackmail, extortion, identity theft, fraud, and any number of additional harms for the rest of his life. He also experienced great stress upon learning of the fraudulent tax return.

137. As a direct and proximate result of the Data Breach, Plaintiff Bauer suffered actual injury and damages from having his PII compromised including, but not limited to: (a) identify theft; (b) damage to and diminution in the value of his PII; (c) loss of value, privacy, and confidentiality of his PII; (d) the cost of indefinite monitoring and protection of his financial accounts; (e) violation of his privacy rights; (f) loss of time; and (g) failure to receive the benefit of his bargain.

138. Plaintiff Bauer has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

d. *Plaintiff Elizabeth Golec*

139. Plaintiff Golec is a former student at Hofstra University. She then transferred to Rhode Island College, where she completed her bachelor's degree.

140. For purposes of receiving educational services from Hofstra University and Rhode Island College, Plaintiff Golec was required to provide her highly sensitive information, including her PII and financial account information to Hofstra University and Rhode Island College and/or Defendant.

141. On information and belief, Hofstra University and Rhode Island College provided Plaintiff Golec's PII and financial account information to Defendant in connection with the services Hofstra University and Rhode Island College provides to Plaintiff Golec.

142. As a result of the Data Breach, Plaintiff Golec received a notice informing her that her PII had been accessed by unauthorized individuals in the Data Breach.

143. In late January 2024, Plaintiff Golec was notified that her Private Information was posted on the dark web. As a result, Plaintiff Golec placed freezes on her accounts.

144. Plaintiff Golec takes care in protecting her PII from disclosure. In light of the multiple prior instances of identity theft and the continued risk of the unauthorized use of her PII, she is now forced to monitor her accounts for signs of fraud and identity theft and to devote valuable time and resources to the same.

145. Plaintiff Golec suffered emotional distress knowing that her highly personal information is no longer confidential and can be used for blackmail, extortion, identity theft, fraud, and any number of additional harms for the rest of her life.

146. As a direct and proximate result of the Data Breach, Plaintiff Golec suffered actual injury and damages from having her PII compromised including, but not limited to: (a) damage to and diminution in the value of her PII; (b) loss of value, privacy, and confidentiality of her PII; (c) the cost of indefinite monitoring and protection of her financial accounts; (d) violation of her privacy rights; (e) loss of time; and (f) failure to receive the benefit of her bargain.

147. Plaintiff Golec has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

e. *Plaintiff Alexys Taylor*

148. Plaintiff Taylor is a current student at Calvin University.

149. For purposes of receiving educational services from Calvin University, Plaintiff Taylor was required to provide her highly sensitive information, including her PII and financial account information to Calvin University and/or Defendant.

150. On information and belief, Calvin University provided Plaintiff Taylor's PII and financial account information to Defendant in connection with the services Calvin University provides to Plaintiff Taylor.

151. As a result of the Data Breach, Plaintiff Taylor received a notice informing her that her information had been accessed by unauthorized individuals in the Data Breach. Specifically, information pertaining to a Form 1098-E or Form 1098-T that she had previously received, and which pertained to her student loans. This document included information such as her name, financial information, and Social Security number.

152. Additionally, on multiple instances from December 2023 through August 2024, Plaintiff Taylor has received notifications of unauthorized credit inquiries and attempts to open accounts using her PII.

153. Plaintiff Taylor takes care in protecting her PII from disclosure. In light of the multiple prior instances of identity theft and the continued risk of the unauthorized use of her PII, she is now forced to monitor her financial accounts for signs of fraud and identity theft and to devote valuable time and resources to the same.

154. Plaintiff Taylor suffered emotional distress knowing that her highly personal information is no longer confidential and can be used for blackmail, extortion, identity theft, fraud, and any number of additional harms for the rest of her life.

155. As a direct and proximate result of the Data Breach, Plaintiff Taylor suffered actual injury and damages from having her PII compromised including, but not limited to: (a) damage to and diminution in the value of her PII; (b) loss of value, privacy, and confidentiality of her PII; (c) the cost of indefinite monitoring and protection of her financial accounts; (d) violation of her privacy rights; (e) loss of time; and (f) failure to receive the benefit of her bargain.

156. Plaintiff Taylor has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

157. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as:

All individuals in the United States and its territories whose PII was compromised in the ECSI Data Breach (the "Class").

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

159. Plaintiffs reserve the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

160. **Numerosity.** Plaintiffs are informed and believe, and thereon allege, that there are, at minimum, hundreds of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through ECSI's records, including but not limited to the files implicated in the Data Breach, but based on public information about the number of colleges and universities that provide PII to Defendant, the Class includes hundreds of thousands of individuals.

161. **Commonality.** This action involves questions of law and fact that are common to the Class Members:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' PII;
- c. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
- d. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;
- e. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;
- f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII;
- g. 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;

- h. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- i. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and
- j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

162. **Typicality.** Plaintiffs' claims are typical of the claims of the Class Members. The claims of Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard their PII. Plaintiffs and Class Members directly or indirectly entrusted Defendant with their PII, and it was subsequently obtained by an unauthorized third party.

163. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for themselves and for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs have also retained counsel that is competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

164. **Superiority.** Class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class Member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale,

and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

165. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, ECSI's liability and the fact of damages is common to Plaintiffs and each member of the Class. If ECSI breached its duties, then Plaintiffs and each Class Member suffered damages by that conduct.

166. **Injunctive and Declaratory Relief.** Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

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

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs restate and reallege the foregoing allegations as if fully set forth herein.

169. ECSI owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and otherwise handling their PII and protect it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

170. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's security systems to ensure that Plaintiffs' and Class Members' PII in

ECSI's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

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

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

173. ECSI also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiffs and Class Members.

174. ECSI also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach in the financial sector.

175. ECSI also owed a duty to Plaintiffs and Class Members pursuant to Section 5 of the FTC Act.

176. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as ECSI for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duties.

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

178. ECSI breached these duties owed to Plaintiffs and Class Members and thus was negligent. ECSI breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies provided to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

179. But for ECSI's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been accessed and exfiltrated by cybercriminals.

180. As a direct and proximate result of ECSI's negligence, Plaintiffs and Class Members have suffered injuries including:

- a. Theft of their PII;
- b. Misuse of their PII;
- c. Identity theft;

- d. Costs associated with requesting credit freezes;
- e. Costs associated with the detection and prevention of identity theft;
- f. Costs associated with purchasing credit monitoring and identity theft protection services;
- g. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- h. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;
- i. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- j. Damages to and diminution in value of their PII entrusted to ECSI with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and
- k. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members.

181. As a direct and proximate result of ECSI's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs restate and reallege the foregoing allegations as if fully set forth herein.

183. Through its course of conduct, Defendant entered into implied contracts with Plaintiffs and Class Members for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII and financial information.

184. Defendant required Plaintiffs and Class Members to provide and entrust their PII and financial information as a condition of obtaining Defendant's services.

185. Defendant solicited and invited Plaintiffs and Class Members to provide their PII and financial information as part of Defendant's regular business practices.

186. Plaintiffs and Class Members accepted Defendant's offers and provided their PII and financial information to Defendant.

187. As a condition of their relationship with Defendant, Plaintiffs and Class Members provided and entrusted their PII and financial information to Defendant.

188. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached, compromised, or stolen.

189. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII and financial information to Defendant, in exchange for, among other things, the protection of their PII and financial information.

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

191. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their PII and financial information and by failing to provide timely and accurate notice to them that their PII and financial information was compromised as a result of the Data Breach.

192. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered and will continue to suffer: (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost time spend monitoring financial accounts and credit; and (f) other economic and non-economic harm.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

193. Plaintiffs restate and reallege the foregoing allegations as if fully set forth herein.

194. Plaintiffs bring this claim in the alternative to the breach of implied contract claim, to the extent that a contract does not exist between the parties.

195. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiffs and Class Members.

196. Defendant, prior to and at the time Plaintiffs and Class Members entrusted their PII and financial information to Defendant, caused Plaintiffs and Class Members to reasonably believe that Defendant would keep such PII and financial information secure.

197. Defendant was aware, or should have been aware, that reasonable consumers would have wanted their PII and financial information kept secure and would not have contracted with

Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

198. Defendant was also aware that, if the sub-standard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiffs' and Class Members' decisions to seek services therefrom or from its clients.

199. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information from it and its clients.

200. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiffs and Class Members the ability to make a rational and informed purchasing and servicing decision and took undue advantage of Plaintiffs and Class Members.

201. Defendant was unjustly enriched at the expense of Plaintiffs and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs and Class Members; however, Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and services that did not satisfy the purpose for which they paid.

202. Since Defendant's profits were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation, or profits it realized from these transactions.

203. Plaintiffs and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits obtained by Defendant from its wrongful

conduct or establish a constructive trust from which Plaintiffs and Class Members may seek restitution.

FOURTH CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

204. Plaintiffs restate and reallege the foregoing allegations as if fully set forth herein.

205. Plaintiffs and Class Members had a legitimate expectation of privacy in their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

206. ECSI owed a duty to Plaintiffs and Class Members, to keep their PII confidential.

207. ECSI failed to protect, and allowed unknown and unauthorized third parties to access, the PII of Plaintiffs and Class Members.

208. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential.

209. ECSI acted with reckless disregard for the privacy of Plaintiffs and Class Members rising to the level of: (a) an intentional intrusion by Defendant; (b) into a matter that Plaintiffs and Class Members have a right to keep private (*i.e.*, their PII); and (c) which is highly offensive to a reasonable person.

210. ECSI acted knowingly when it permitted the Data Breach to occur; it knew that it was designing a system that would permit individuals to access Plaintiffs' and Class Members' highly sensitive and confidential PII without requiring the user to log in or require adequate identity confirmation, such that its data security practices were inadequate and insufficient.

211. ECSI was aware of the potential of a data breach and failed to implement reasonable procedures to protect the PII on its tax services website, when it knew or should have known that

it was unequipped to prevent the unauthorized release of Plaintiffs' and Class Members' data and PII.

212. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members would be highly offensive to a reasonable person.

213. Plaintiffs and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

214. Plaintiffs restate and reallege the foregoing allegations as if fully set forth herein.

215. 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 laws and regulations described herein.

216. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether ECSI is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that ECSI still possess Plaintiffs' and Class Members' PII, and that ECSI's data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

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

- a. ECSI owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

- b. ECSI continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiffs' and Class Members' PII still in its possession.

218. This Court also should issue corresponding prospective injunctive relief requiring ECSI to employ adequate security protocols consistent with law and industry standards to protect consumers' PII in its possession.

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

220. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to ECSI if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to ECSI of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

221. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at ECSI, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

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

- A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;
- B. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;
- C. For damages in an amount to be determined by the trier of fact;
- D. For an order of restitution and all other forms of equitable monetary relief;
- E. Declaratory and injunctive relief as described herein;
- F. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;
- G. Awarding pre- and post-judgment interest on any amounts awarded; and
- H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: September 13, 2024

Respectfully submitted,

/s/ Nicholas A. Colella

Nicholas A. Colella (PA 332699)

LYNCH CARPENTER, LLP

1133 Penn Ave., 5th Floor

Pittsburgh, PA 15222

Telephone: (412) 322-9243

nickc@lcllp.com

Nickolas J. Hagman (*pro hac vice*)

**CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP**

135 S. LaSalle, Suite 3210

Chicago, Illinois 60603

Telephone: (312) 782-4880

Facsimile: (312) 782-4485

nhagman@caffertyclobes.com

Plaintiffs' Co-Lead Interim Counsel