IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

MICHAEL EVANGELISTA, individually and on behalf of himself and all others similarly situated, Plaintiff, v. **NATIONAL STUDENT CLEARINGHOUSE** and **PROGRESS SOFTWARE CORPORATION**, Defendants.	Civil Action No.: _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Michael Evangelista ("Plaintiff"), individually on behalf of himself and all others similarly situated, alleges the following against National Student Clearinghouse ("the Clearinghouse" or "NSC") and Progress Software Corporation ("PSC") (collectively, "Defendants") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' highly sensitive personal information, including but not limited to: names; dates of birth; contact information; Social

Security numbers; student ID numbers; and certain school-related records such as, enrollment records, degree records, and course-level data (the "Private Information" or "PII").

2. PSC is a software company offering a range of products and services to government and corporate entities across the country and around the world, including cloud hosting and secure file transfer services such as MOVEit file transfer and MOVEit cloud.

3. PSC provides its MOVEit file transfer software to numerous commercial and governmental entities, including NSC, to support the transfer of sensitive data files.[1]

4. NSC claims to be the leading provider of educational reporting, verification, and research services for North American colleges and universities, providing these services to approximately 3,600 colleges and universities.[2] NSC also provides similar services to approximately 22,000 high schools.[3] And NSC provides services directly to students.[4]

5. Between May 27 and May 31, 2023, the notorious CL0P ransomware gang exploited a vulnerability in the MOVEit technology during a massive cyberattack, during which the cybercriminals accessed and exfiltrated Plaintiff's and Class Members' Private Information stored therein (the "Data Breach").

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a (last accessed 10/10/23).
[2] https://www.bleepingcomputer.com/news/security/national-student-clearinghouse-data-breach-impacts-890-schools/; https://www.studentclearinghouse.org/about/. (accessed 10/03/2023)
[3] https://www.studentclearinghouse.org/about/. (accessed 10/03/2023)
[4] *Id*. ("The National Student Clearinghouse® offers convenient online services for students. From here, you can order transcripts, obtain verification of your in-school status, find money-saving student discounts, and more. As the trusted partner of your educational institutions, all our services are offered with your security and privacy in mind.").

6. Investigations following CL0P's exploitation of the MOVEit vulnerability have subsequently revealed that CL0P had known about this particular vulnerability and had been experimenting with ways to exploit as far back as 2021.[5]

7. Indeed, one security firm's review of "logs of impacted [MOVEit] clients found evidence of similar [malicious] activity occurring in multiple client environments last year (April 2022) and in some cases as early as July 2021."[6]

8. The security firm "also discovered the threat actors were testing ways to collect and extract sensitive data from compromised MOVEit Transfer servers as far back as April 2022, likely with the help of automated tools."[7]

9. On or about May31, 2023, NSC was informed by PSC of the Data Breach.[8]

10. After PSC notified NSC of the Data Breach, NSC initiated an investigation which concluded that during the Data Breach, CL0P was able to exfiltrate certain files from the MOVEit file transfer software related to approximately 890 schools for which NSC provides its services .[9]

11. On August 31, 2023, over two months after NSC confirmed that it was the subject of the Data Breach, NSC sent direct notice to those individuals impacted by the Data Breach. These

[5] Laurie Iacono et al., *Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, KROLL (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.
[6] Sergiu Gatlan, *Clop Ransomware Likely Testing MOVEit Zero-Day Since 2021*, BLEEPING COMPUTER (June 8, 2023), https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/.
[7] *Id.*
[8] Torres, Ricardo D. "Notice of Data Breach". The National Student Clearinghouse. August 31, 2023.
[9] *Id.*

delays gave cyber criminals a head start on using Plaintiff's and the Class's PII for nefarious, commercial purposes.[10]

12. On September 26, 2023, Plaintiff finally received the "Notice of Data Breach" via U.S. Mail from NSC.

13. The Private Information compromised in the Data Breach includes highly sensitive data that represents a gold mine for data thieves. Armed with the Private Information accessed in the Data Breach, data thieves can and likely have committed a variety of crimes and bad acts including, *e.g.*, opening new financial accounts in the Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, and filing fraudulent tax returns using Class Members' information.

14. Plaintiff and the Class entrusted their PII to NSC, who then provided their PII to PSC. ***Both*** Defendants willingly accepted the responsibility to adequately secure, safeguard, and maintain the PII of Plaintiff and the Class.

15. On its website, NSC proclaims its commitment to securing the data of students, including Plaintiff and Class Members, each of whom entrusted NSC with their PII. NSC states:

> "The National Student Clearinghouse collects data on student enrollment, academic progress, and educational outcomes to help educational institutions accomplish their missions. ***Our work – performed in a trusted, secure, and private environment*** – provides numerous time- and cost-saving benefits to students, schools, administrators, and requestors.
>
> ***Our education partners trust the Clearinghouse because they know we take our commitment to student privacy very seriously. We have maintained confidentiality and privacy of the student records in our care. We are scrupulous in our concern for student privacy and compliance with the Family Educational Rights and Privacy Act (FERPA), which protects students' privacy rights in their education records.***

[10] *Id.*

> ***We understand the way we collect, use, and share those data has powerful implications for diversity, equity, and inclusion (DEI) in education and the workforce.***"[11]

16. Similarly, on its website, PSC represented that its MOVEit file transfer software would "Transfer Sensitive Information Securely – Encryption in-transit and at-rest and advanced security features keep sensitive information out of harm's way."[12]

17. Nevertheless, Defendants patently disregarded their own stated policies and procedures and the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement or maintain adequate and reasonable data security measures and ensure those measures were followed by themselves and by their Information Technology ("IT") vendors to ensure that the PII of Plaintiff and Class Members was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was exfiltrated from the MOVEit file transfer software by cybercriminals. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and therefore they are entitled to damages and injunctive relief and other equitable relief as a result of Defendants' failures.

18. Plaintiff brings this class action lawsuit to address Defendants' inadequate safeguarding of Plaintiff's and Class Members' Private Information and Defendants' failure to provide timely and adequate notice to Plaintiff and Class Members of, among other things, the occurrence of the Data Breach, that their Private Information was subject to unauthorized access by cybercriminals, the types of information that were accessed, what if anything was being done

[11] https://www.studentclearinghouse.org/dei-data-lab/about/about-our-data/ (emphasis added.)
[12] https://www.progress.com/moveit

to protect Plaintiff and Class Members and the stolen information, and what if anything Plaintiff and Class Members could or should do to protect themselves and their information going forward.

19. The improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Defendants. Specifically, NSC knew that if it did not select a vendor with adequate data security that Plaintiff's and the Class's PII would be targeted by cybercriminals. Indeed, NSC coauthored a "white paper" (hereafter, the "NSC White Paper") concerning cybersecurity in which it labeled third-party vendors a "[r]isk in plain sight", and warned that "third-party vendors are a significant potential risk to [educational institutions' and students'] data security" and "[s]tudent data is only as secure as that third-party vendor".[13] Similarly, discovery will show that PSC was on notice that failing to take necessary steps to secure the PII it possessed left its clients' vulnerable to an attack and put Plaintiff's and Class Member's PII at risk of unauthorized access or compromise.

20. Upon information and belief, PSC failed to properly monitor its networks and systems and failed to properly implement adequate data security practices, procedures, infrastructure, and protocols with regard to the computer network and systems that housed PII. Had PSC properly monitored and secured its networks, the Data Breach would not have happened.

[13] The NSC White Paper, titled "Why Cybersecurity Matters: and What Registrars, Enrollment Managers and Higher Education Should Do About It, is attached hereto as Exhibit 1. The NSC White Paper states that, "A good example of potential third-party vulnerability arises from contracts with companies that market their services … purporting to streamline the office's workload by taking over some process or service." Ironically, this is one of the benefits NSC touts to using its services. *See, e.g.*, NSC "Fact Sheet" attached hereto as Exhibit 2, at p. 1 ("Adoption of Clearinghouse back-office services allows individual states to reallocate employees system wide (as many as 100 or more, in some cases) to other important student-focused tasks.") and p. 2 ("Our education partners TRUST the Clearinghouse and realize substantial savings and productivity gains through redeployment of administrative resources.")

21. Upon information and belief, NSC failed to properly inquire about PSC's data security before entrusting it with Plaintiff's and the Class's PII, and failed to monitor and oversee PSC's data security throughout their relationship. Had NSC properly inquired about PSC's data security, oversaw PSC's data security, and monitored PSC's data security, Plaintiff's and the Class's PII would not have been exfiltrated by cybercriminals.

22. Plaintiff and Class Members now face a substantially increased and certainly impending risk of identity theft and fraud as a result of Defendants' negligent conduct as Plaintiff's and Class Members' PII that Defendants collected and maintained is now in the hands of cyber criminals..

23. Plaintiff seeks to remedy these harms on behalf of himself and all other similarly situated individuals whose PII was accessed and/or compromised during the Data Breach.

PARTIES

24. Plaintiff Michael Evangelista is, and at all times mentioned herein was, an individual resident and citizen of the State of Georgia, County of Pickens.

25. Defendant PSC is a secure file transfer services software company with its principal place of business located at 15 Wayside Rd, Suite 400, Burlington, Massachusetts 01803, and is incorporated in the Commonwealth of Massachusetts. PSC is registered as a foreign corporation in the Commonwealth of Virginia and maintains a registered agent in Richmond, Virginia.

26. Defendant NSC provides educational reporting and verification services to educational institutions, students and alumni, employers, and other organizations. NSC is a Virginia non-profit corporation with a principal place of business located at 2300 Dulles Station Blvd., Suite 220, Herndon, Virginia 20171.

JURISDICTION AND VENUE

27. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, as at least one member of the plaintiff Class and at least one Defendant are citizens of different states, the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interests and costs, and there are 100 or more members of the Class.

28. This Court has personal jurisdiction over NSC because its principal place of business is located in the Eastern District of Virginia; NSC is authorized to and regularly conducts business in the Eastern District of Virginia; and a substantial part of the acts and omissions giving rise to this action occurred in this District.

29. This Court has personal jurisdiction over PSC because it is authorized to and regularly conducts business in the Eastern District of Virginia, and a substantial part of the acts and omissions giving rise to this action occurred in this District.

30. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because NSC is a Virginia corporation, has its principal place of business in this District and in this Division, and a substantial part of the events and omissions giving rise to this action occurred in this District and in this Division.

FACTUAL ALLEGATIONS

A. Defendants' Business and Collection of Plaintiff's and Class Members' Private Information

31. PSC is a software company offering a range of products and services to government and corporate entities across the country and around the world, including cloud hosting and secure file transfer services such as MOVEit file transfer and MOVEit cloud. NSC engaged PSC as a vendor and/or third-party contractor to provide it with the MOVEit file transfer software.

32. NSC provides educational reporting and verification services to educational institutions, students and alumni, employers, and other organizations.

33. Upon information and belief, as a condition of providing its products and/or services, NSC requires that individuals, including Plaintiff and Class Members, directly or indirectly provide and entrust it with highly sensitive personal information. The information is then held or transferred by Defendants in their computer systems that were compromised at the time of the Data Breach.

34. NSC collects and stores the highly sensitive PII of Plaintiff and the Class.[14] Upon information and belief, NSC discloses the PII it receives from Plaintiff and the Class to PSC to utilize PSC's MOVEit software. Thus, PSC requires NSC to entrust it with highly sensitive personal information belonging to individuals such as Plaintiff and the Class.

35. Because of the highly sensitive and personal nature of the information PSC and NSC collect, acquire, and store, Defendants assumed equitable and legal duties that include among other things: keeping Plaintiff's and the Class's PII private; complying with industry standards related to data security; only using and releasing highly sensitive information stored on their servers for reasons that relate to the services they provide; and providing timely and adequate

[14] *See* https://www.studentclearinghouse.org/privacy-policy/ ("The Clearinghouse collects education records, which include both Directory and Non-Directory Information, from Participating Institutions, education agencies, and other education authorities, under either the school official or directory information exceptions to the Family Educational Rights and Privacy Act ("FERPA"). With this delegated authority, the Clearinghouse uses this data for enrollment reporting of Title IV schools to the National Student Loan Data System ("NSLDS"), enrollment reporting to private lenders, verification of student enrollment and credentials earned, transcript services, course exchange, and research."); *see also* Exhibit 2, at p. 2 ("The Clearinghouse captures data from all types and sizes of institutions (e.g., public, private, 2-/4-year, nonprofit/for-profit) ….).

notice to individuals to whom that information belongs if their Private Information is disclosed without authorization.

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

B. The Data Breach and Defendants' Inadequate Notice to Plaintiff and Class Members

37. During the Data Breach, CL0P was able to gain access and ultimately exfiltrate a cache of highly sensitive personal information, including but not limited to names, dates of birth, contact information, Social Security numbers, Student ID numbers, and school related records (such as enrollment records, degree records, and course-level data).

38. The PII accessed in the Data Breach cannot be easily replaced or changed by Plaintiff and Class Members.

39. Defendants had obligations created by contract, industry standards, common law, and by representations made to Plaintiff and Class Members, to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.[15]

40. Plaintiff and Class Members directly or indirectly provided their Private Information to Defendants with the reasonable expectation and mutual understanding that

[15] See, e.g., https://www.studentclearinghouse.org/about/our-privacy-commitment/ ("Our education partners trust the National Student Clearinghouse® because they know we take our commitment to student privacy very seriously. We have maintained the confidentiality and privacy of the student records in our care since our beginning in 1993. We are scrupulous in our concern for student privacy and compliance with the Family Educational Rights and Privacy Act (FERPA), which protects students' privacy rights in their education records.")

Defendants would comply with their obligations to keep such Private Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

41. Plaintiff and the Class also directly or indirectly provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would not hand over their PII to a vendor with inadequate data security and would continue to ensure their PII was being protected by, among other things, monitoring and overseeing the vendors to which they gave access to Plaintiff's and the Class's PII.

42. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cyber gang, CL0P.[16] Indeed, NSC expressly acknowledged in the NSC White Paper that "Universities and colleges collect a wide variety of personal information about their students, including Social Security numbers, birth dates, financial information, and contact information. … [A]dvanced, organized networks of cyberspies, which are sponsored by other countries, are actively targeting higher education institutions …. (Exhibit 1, p. 3.)

43. Thus, Defendants knew or should have known that the MOVEit software and electronic records and PII transferred therein would be targeted by cybercriminals.

C. Defendants Failed to Comply with FTC Guidelines

44. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-

[16] *See* https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware- gang/; *see also* https://www.bleepingcomputer.com/news/security/fortra-shares- findings-on-goanywhere-mft-zero-day-attacks/.

making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair act or practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

45. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to detect a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

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

48. Upon information and belief, PSC and NSC failed to properly implement basic data security practices recommended by the FTC. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

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

D. Defendants Failed to Comply with Industry Standards

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

51. Industry best practices should be implemented by businesses like Defendants. "All of us in higher education have a vested interest in knowing cybersecurity best practices and being empowered to effectively navigate the myriad of cyber security challenges."[17] Best Practices include but are not limited to educating all employees, implementing strong password requirements, instituting multilayer security including firewalls, employing anti-virus and anti-malware software, encrypting consumer data when at rest, utilizing multi-factor authentication, backing up data, limiting which employees can access sensitive data, and properly selecting and monitoring third-party vendors. Upon information and belief, Defendants failed to follow one or more of these industry best practices.

52. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports;

[17] NSC White Paper, p. 2.

protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff and customers regarding these points. Upon information and belief, Defendants failed to follow one or more of these cybersecurity best practices.

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

54. Upon information and belief, the Data Breach was proximately caused by Defendants' failure to comply with accepted standards.

E. Defendants Breached Their Duties to Safeguard Plaintiff's and Class Members' Private Information

55. In addition to their obligations under federal and state laws, PSC and NSC owed common law duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

56. PSC owed a duty to Plaintiff and Class Members to provide reasonable data security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

57. NSC owed a duty to Plaintiff and Class Members to safeguard their PII and ensure any vendor/contractors/third parties it hired maintained adequate data security. This duty also required NSC to oversee and monitor all vendor/contractors/third parties it hired.

58. Defendants breached their duties and obligations owed to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard Plaintiff's and the Class's PII. Defendants' improper, actionable and unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. PSC and NSC failing to adequately protect Plaintiff's and the Class's Private Information;

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

d. NSC failing to properly oversee and monitor PSC;

e. NSC failing to ensure PSC had adequate data security prior to entering into a contractual relationship with PSC;

f. PSC failing to sufficiently train its employees regarding the proper handling of its customers' files containing the Private Information;

g. Defendants failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

h. Defendants failing to adhere to industry standards for cybersecurity as discussed above; and

i. Defendants otherwise breaching duties and obligations to protect Plaintiff's and Class Members' Private Information.

59. NSC negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing a third-party with inadequate data security, PSC, access to Plaintiff's and the Class's PII and by failing to oversee and monitor PSC and its data security throughout the course of their relationship.

60. PSC negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network, systems, and servers which, upon information and belief, contained unsecured and unencrypted Private Information.

61. Had PSC remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

62. Had NSC properly vetted PSC before retaining PSC's services and adequately monitored and oversaw PSC, it could have prevented the exposure of Plaintiff's and Class Members' PII in the Data Breach because it never would have been in the hands of PSC to begin with.

63. As a direct and proximate result of the acts and omissions of Defendants as set forth herein, Plaintiff's and Class Members' lives were severely disrupted. Plaintiff and Class Members have been harmed because of the Data Breach and face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants.

F. Defendants Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft

64. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[18] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Moreover, consumers' loss of trust in e-commerce deprives them of the benefits provided by the full range of goods and services available, with attendant negative impacts on daily life.

65. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Indeed, CL0P has already extorted companies victimized by the MOVEit data theft.[19]

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

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

[19] *See* https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-starts-extorting-moveit-data-theft-victims/.

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

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

68. Thus, even if certain information was not purportedly involved in the Data Breach, unauthorized parties could use Plaintiff's and Class Members' Private Information to obtain or link with other information and access accounts such as email accounts and even financial accounts to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

69. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[20]

70. These steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts. Identity thieves can and often do use stolen personal

---

20 S*ee IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps.

information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank fraud to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. Manifestly, PII has considerable market value. PII can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which can include heavy prison sentences for perpetrators). The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[21]

72. The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

73. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[22] Experian reports that a stolen credit or debit card number can

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

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

sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[23]

74. The value of PII is increasingly evident in our digital economy. Many companies collect PII for purposes of data analytics and marketing. These companies collect it to better target customers and share it with third parties for similar purposes.[24]

75. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[25]

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

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

---

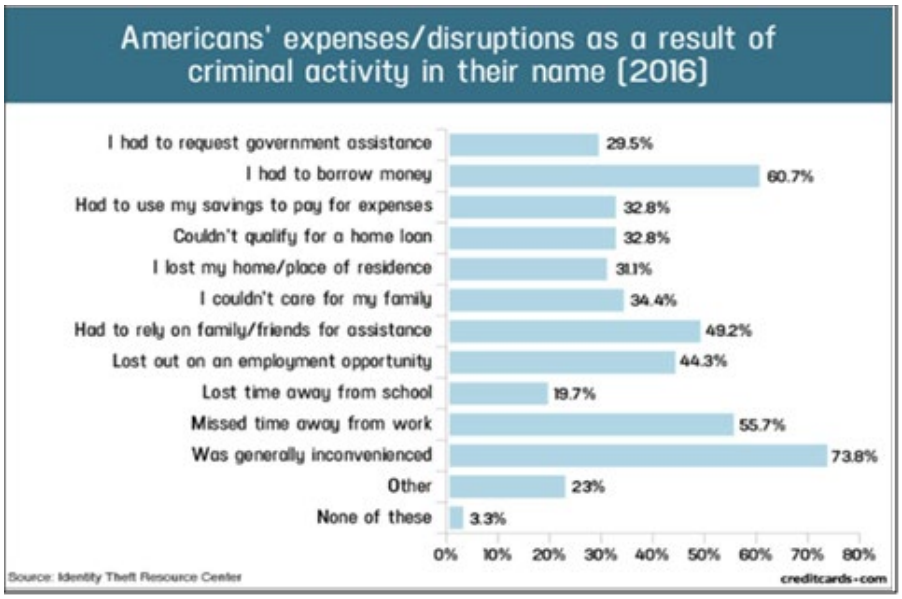
[23] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the- dark-web/.

[24] *See* https://robinhood.com/us/en/support/articles/privacy-policy/.

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

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

79. A study by the Identity Theft Resource Center[26] shows the multitude of harms caused by fraudulent use of PII:



80. The NSC White Paper expressly recognizes the costs, damages and other harms suffered by students whose PII has been disclosed improperly:

> The most important cost to keep in mind is the long-term cost that students face after they have had their personal information stolen. Students trust their institutions to be diligent stewards of their data. Once the organization has been breached, however, there is no real way to make amends. **The genie is out of the bottle, and the data is not coming back**.
> Students affected by cybersecurity breaches face significant short-term inconveniences that can translate to lifelong negative effects if their data is used. Students may have to:

- Change passwords across their accounts
- Request their credit reports
- Establish fraud alerts on their credit files

[26]Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *availa ble at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/.

- Freeze their credit reports
- Dispute fraudulent activity
- Contact financial institutions
- Enroll in identity monitoring services
- Complete police reports
- Submit formal identity theft reports to the Federal Trade Commission (FTC)

> If a student's identity is stolen as a result of a data breach, that student faces even greater challenges. The student's credit reports could be affected, and student loans might be delayed or canceled.

Exhibit 1, p. 5 (emphasis added).

81. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[27]

> [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.

PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

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

G. *Plaintiff Evangelista's Experiences*

82. Plaintiff Evangelista is a resident and citizen of the State of Georgia and was required to directly or indirectly provide his PII to NSC. Thus, NSC acquired, collected, and stored Plaintiff's PII.

83. In May of 2023, Plaintiff Evangelista graduated from one of the colleges that used NSC's services. Plaintiff Evangelista later received a letter from NSC informing him that his PII had been compromised during the Data Breach. As a result of the Data Breach, Plaintiff Evangelista is very concerned as he is currently applying for full-time employment where many of the prospective employers run background and credit checks. Plaintiff Evangelista worries that his compromised data might affect future employment prospects.

84. By virtue of NSC's relationship with PSC, PSC also acquired, collected, and stored Plaintiff's PII through NSC's use of the MOVEit software services .

85. Defendants were in possession of Plaintiff Evangelista's PII before, during, and after the Data Breach.

86. Defendants were obligated by law, regulations, and guidelines to protect Plaintiff Evangelista's PII and NSC was required to ensure PSC maintained adequate data security, infrastructure, procedures, and protocols for Plaintiff's PII.

87. As a direct and traceable result of the Data Breach, Plaintiff Evangelista has spent approximately ***20 hours*** addressing the fallout of the Data Breach. Specifically, Plaintiff Evangelista has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: (i) researching the Data Breach; (ii) reviewing credit reports and financial account statements for fraud; (iii) researching credit monitoring and identity theft protection services; and (iv) purchasing, with his own funds, additional credit monitoring as a result of the Data Breach.

This is valuable time Plaintiff Evangelista would have otherwise spent on other activities, including, but not limited to, work, recreation, or time with his family. However, this is not the end. Plaintiff Evangelista will now be forced to, among other things, expend additional time to review his credit reports and monitor his accounts for the rest of his life.

88. Plaintiff Evangelista places significant value on the security of his PII and does not readily disclose it. Plaintiff Evangelista directly or indirectly entrusted his PII to Defendants with the understanding that Defendants would keep his information secure and that Defendants would employ reasonable and adequate security measures to ensure that his PII would not be compromised.

89. Likewise, Plaintiff Evangelista directly or indirectly entrusted his PII to NSC with the understanding that NSC would not hire entities to provide technology services that did not employ adequate data security, such as PSC.

90. As a direct and traceable result of the Data Breach, Plaintiff Evangelista suffered actual damages to include: (i) lost time related to monitoring his accounts for fraudulent activity; (ii) loss of privacy due to his PII being stolen by cybercriminals; (iii) loss of the benefit of the bargain because Defendants did not adequately protect his PII; (iv) the loss in value of his PII due to his PII being in the hands of cybercriminals who can use it at their leisure; and (v) other economic and non-economic harm.

91. Also, as a direct and traceable result of the Data Breach, Plaintiff Evangelista has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

92. As a result of the Data Breach, Plaintiff Evangelista has suffered emotional distress due to the release of his PII, due to the fact that he believed Defendants would protect his PII from unauthorized access and disclosure, but utterly failed to do so. Plaintiff Evangelista has suffered anxiety about unauthorized parties viewing, selling, and/or using his Personal Information for purposes of identity theft and fraud. Knowing that thieves intentionally targeted and stole his PII, and knowing that his PII is likely available on the dark web, has caused Plaintiff Evangelista great anxiety beyond mere worry. Specifically, Evangelista is in a state of persistent worry now that his PII has been exposed in the Data Breach. Plaintiff Evangelista remains very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. Plaintiff Evangelista has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendants, is protected and safeguarded from future data breaches and unauthorized and improper and unlawful use.

H. *Plaintiff's and Class Members' Damages*

94. Plaintiff and the Class have suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach, among the damages described above.

95. Plaintiff and the Class would not have provided their PII to NSC had NSC disclosed it would surrender their PII to a third-party with inadequate data security, such as PSC, and would not oversee or monitor PSC once their PII was transferred to PSC.

96. Additionally, Plaintiff and the Class would not have permitted their PII to be provided to NSC and then to PSC had NSC and/or PSC timely disclosed that PSC's file transfer

software lacked adequate data security to safeguard their PII which was exposed in the Data Breach.

97. Plaintiff and the Class suffered actual injury in the form of having their Private Information compromised and/or stolen as a result of the Data Breach. Plaintiff and the Class suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that Plaintiff and the Class entrusted to the Clearinghouse.

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

100. Plaintiff and the Class have a continuing interest in ensuring that their Private Information, which remains in Defendants' possession and stored within Defendants' systems, is protected, and safeguarded from future breaches and third parties with inadequate data security.

101. As a result of the Data Breach, Plaintiff and the Class have already made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching long-term credit monitoring options they will now need to use.

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

103. Plaintiff's and the Class's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from NSC's failure to ensure the third-party it hired had adequate data security, from NSC's failure to oversee and monitor the third-party it hired, and from PSC's inadequate data security practices.

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

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

106. The Private Information maintained by and stolen from Defendants, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

107. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs as a result of the Data Breach.

108. NSC has offered only two years of credit monitoring services, which is neither adequate nor sufficient protection to ensure that Plaintiff's and Class Members' PII will be protected as Plaintiff's and Class Members' PII has been indefinitely exposed. According to

NSC's data breach notice, "We have arranged to offer identity monitoring services. . . for two years."[28]

109. NSC further puts the onus on Plaintiff and Class Members to protect themselves from identity theft and fraud as a result of Defendants' Data Breach, suggesting that they "remain vigilant by reviewing [their] account statements and monitoring [their] free credit for suspicious activity."[29]

110. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

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

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

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

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

[28] "Notice of Data Breach," the National Student Clearinghouse, August 31, 2023
[29] *Id.*

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

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

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

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

CLASS ACTION ALLEGATIONS

112. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure.

113. Specifically, Plaintiff seeks to represent the following Nationwide Class ("Class" or "Class Members"), subject to amendment as appropriate:

> All individuals who reside in the United States whose Private Information was exposed in the Data Breach involving NSC and PSC.

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

115. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

116. The proposed Class meets the criteria for certification.

117. **Numerosity**. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class likely consists of millions of individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through the records of NSC and PSC.

118. **Commonality**. There are questions of law and fact common to the Class which include, without limitation:

a. Whether PSC and NSC engaged in the acts and omissions alleged herein;

b. When PSC and NSC learned of the Data Breach;

c. Whether PSC's and NSC's response to the Data Breach was adequate;

d. Whether PSC and NSC lost or disclosed Plaintiff's and Class Members' Private Information;

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

f. Whether NSC failed to select a vendor with adequate data security;

g. Whether NSC failed to oversee and monitor PSC;

h. Whether PSC's data security practices related to its secure file transfer services prior to and during the Data Breach complied with applicable data security laws and regulations;

i. Whether PSC's data security practices related to its secure file transfer services prior to and during the Data Breach were consistent with industry standards;

j. Whether PSC and NSC owed a duty to Class Members to safeguard their Private Information;

k. Whether PSC and NSC breached their duties to Class Members to safeguard their Private Information;

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

m. Whether Defendants had a legal duty to provide timely, accurate and sufficient notice of the Data Breach to Plaintiff and the Class Members;

n. Whether Defendants breached their duty to provide timely, accurate and sufficient notice of the Data Breach to Plaintiff and Class Members;

o. Whether PSC and NSC knew or should have known that PSC's data security systems and monitoring processes relate to their secure file transfer services were deficient;

p. What damages Plaintiff and Class Members suffered as a result of Defendants' acts, omissions and misconduct;

q. Whether Defendants' conduct was negligent;

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

s. Whether Defendants were unjustly enriched;

t. Whether Plaintiff and Class Members are entitled to damages;

u. Whether Plaintiff and Class Members are entitled to credit or identity monitoring and monetary relief; and

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

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

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

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

122. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action,

most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PSC. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

123. **Injunctive Relief.** Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final relief, whether it be injunctive, declaratory or monetary, is appropriate as to the Class as a whole.

124. **Ascertainability.** All members of the proposed Class are readily ascertainable. The proposed class definition is based on objective criteria and Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT 1
NEGLIGENCE
(Alleged Against Both Defendants)
(On behalf of Plaintiff and the Nationwide Class)

125. Plaintiff restates and realleges all the allegations stated above as if fully set forth herein.

126. NSC knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding and protecting such Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties. To fulfill this duty of care, NSC was required to ensure that any third parties/contractors/vendors it hired also maintained adequate data security, procedures,

systems, infrastructure, and protocols. NSC was also required to oversee and monitor any and all third parties/contractors/vendors it hired who handled Plaintiff's and the Class's PII.

127. PSC, through its relationship with NSC, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

128. PSC's duty also included a responsibility to implement processes by which it could detect and analyze vulnerabilities of its systems quickly and to give prompt notice to those affected in the case of a cyberattack.

129. PSC and NSC knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate data security. PSC and NSC were each on notice because, on information and belief, they knew or should have known of the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cyber gang, Cl0p.

130. PSC and NSC owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. PSC's and NSC's duties included, but were not limited to, the following:

a. Both Defendants exercising reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. PSC's duty to protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. The Clearinghouse ensuring any vendors or third parties it hired maintained adequate data security;

d. The Clearinghouse overseeing and monitoring any vendors or third parties it hired to ensure it maintained adequate data security throughout the course of the relationship;

e. Defendants' duty to have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

f. PSC's duty to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

g. PSC's duty to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

h. PSC's and the Clearinghouse's duty to promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

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

132. The duties PSC and the Clearinghouse had also arose because Defendants were bound by industry standards to protect confidential Private Information.

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

134. Plaintiff and Class Members were foreseeable victims of any failure of the Clearinghouse to ensure any third party or vendor retained by the Clearinghouse maintained adequate data security, procedures, infrastructure, and protocols before entrusting it with Plaintiff's and the Class's PII. Especially since the Clearinghouse had exclusive control over choosing vendor/third parties/contractors to handle Plaintiff's and the Class's PII.

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

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

137. PSC and the Clearinghouse, by their actions and/or omissions, breached their duties of care by failing to promptly provide direct notice of the Data Breach to the persons whose Private Information was compromised.

138. PSC, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and the vulnerability that caused the Data Breach.

139. PSC and the Clearinghouse breached their duties and were negligent by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. The Clearinghouse failing to ensure all vendor and/or third parties it hired maintained adequate data security procedures, infrastructure, policies, and protocols.

c. The Clearinghouse failing to oversee and monitor the data security procedures, infrastructure, policies, and protocols of the vendors and third parties it hired.

d. PSC failing to adequately monitor the security of its networks and systems;

e. PCS failing to periodically ensure that its email system maintained reasonable data security safeguards;

f. Defendants allowing unauthorized access to Class Members' Private Information;

g. Defendants failing to comply with the FTCA;

h. Defendants failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Defendants failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

140. PSC and the Clearinghouse acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

141. The Clearinghouse had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to turn over their Private Information to the Clearinghouse was predicated on the understanding that the Clearinghouse would take adequate security precautions to protect it, which included ensuring any third parties or vendors the Clearinghouse hired maintained adequate data security. Moreover, only the Clearinghouse had the ability to protect the PII in its possession because Plaintiff and the Class were given no choice as to whether their PII was given to PSC.

142. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

143. As a result of Defendants' ongoing failure to timely notify Plaintiff and Class Members of the Data Breach, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

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

145. As a result of Defendants' negligence in breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their

Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

146. The Clearinghouse and PSC also had independent duties under state laws that required them to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

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

148. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

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

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

COUNT II
NEGLIGENCE PER SE
(Alleged Against Both Defendants)
(On behalf of Plaintiff and the Nationwide Class)

151. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

152. Plaintiff alleges this negligence *per se* theory as alternative to his other negligence claim.

153. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair acts or practices by

Defendants of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendants' duty.

154. Defendants further owed a duty, pursuant to the applicable state laws and regulations such as the Virginia Data Breach Notification Law, to disclose without unreasonable delay any breach of its security systems upon discovery or notification of breach. Virginia Code § 18.2-186.6(B). Under the Virginia statute, notice must go to the Office of the Attorney General and any affected Virginia Resident.

155. Defendants violated Section 5 of the FTCA and the Virginia Data Breach Notification Law, and similar federal[30] and state statutes, by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

156. Plaintiff and members of the Class are consumers within the class of persons Section 5 pf the FTCA and other applicable federal and state laws and regulations were intended to protect.

157. The harm that occurred as a result of Defendants' conduct is the type of harm Section 5 of the FTCA and other applicable federal and state laws and regulations were intended to protect against.

158. Defendants' violation of Section 5 of the FTCA and other applicable federal and state laws and regulations constitutes negligence *per se.*

[30] NSC's website states that it offers "free services, reports, and analytics [to] help institutions meet the growing compliance and assessment requirements associated with state and federal financial aid programs." As such, NSC may be subject to the federal Gramm Leach Bliley Act and its Safeguarding Rules.

159. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses as described herein.

160. Defendants' violative conduct is ongoing in that, upon information and belief, they still hold the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

161. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF CONTRACT
(Alleged Against Both Defendants)
(On behalf of Plaintiff and the Nationwide Class)

162. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

163. Upon information and belief, Defendants entered into a contract(s) whereby PSC agreed to, among other things, provide secure file transfer services to NSC and its customers, which services included adequate data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it (*i.e.*, that of Plaintiff and the Class). In addition, NSC entered into contracts and similar transactions with its customers whereby it agreed to safeguard the Private Information that was to be entrusted to it (*i.e.*, that of Plaintiff and the Class).

164. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that PSC and NSC agreed to receive and protect through their

services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were the intended direct and express beneficiaries of such contracts.

165. Alternatively, the circumstances described herein created an implied contract between PSC and NSC on the one hand, and Plaintiff and Class Members on the other hand, pursuant to which PSC and NSC were obligated to safeguard the Private Information that was to be entrusted to them (*i.e.*, that of Plaintiff and the Class).

166. As described above, by failing to among other things use reasonable data security measures to securely store and transfer the files containing Private Information, PSC breached its contract(s) with NSC, and NSC breached its contract(s) with its customers, and each of PSC and NSC breached its implied contract(s) with Plaintiff and the Class Members.

167. It was foreseeable that Plaintiff and the Class would be harmed by the aforesaid breaches and, indeed, Plaintiff and the Class Members were harmed as described above.

168. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial.

COUNT IV
UNJUST ENRICHMENT
(Alleged Against Both Defendants)
(On behalf of Plaintiff and the Nationwide Class)

169. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

170. Plaintiff and Class Members conferred a benefit on Defendants by surrendering their Private Information to NSC and then to PSC.

171. PSC and NSC derived profits from Plaintiff's and the Class's PII because it allowed them to provide services and derive revenue therefrom.

172. As such, upon information and belief, a portion of the payments made to PSC, which payments would not be possible without Plaintiff and Class Members turning over their Private Information, was to be used to provide a reasonable and adequate level of data security that was in compliance with applicable state and federal laws and regulations and industry standards. However, PSC did not do this. Rather, PSC retained the benefits of its unlawful conduct, including the amounts of payment received that should have been used for adequate cybersecurity practices that it failed to provide.

173. Likewise, upon information and belief, a portion of the payments made to NSC, which payments would not be possible without Plaintiff and Class Members turning over their Private Information, was to be used to provide a vendor and/or contractor with adequate data security. However, NSC did not do this. Instead, NSC retained the benefits of its unlawful conduct, including the amounts of payment received that should have been used for a vendor/contractor/third-party with adequate data security, which it failed to provide.

174. Defendants knew that Plaintiff and Class Members conferred a benefit upon them, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments received to implement adequate data security measures or retain a vendor/contractor/third party with adequate data security, which would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

175. If Plaintiff and Class Members had known that Defendants would not adequately secure their Private Information, they would not have agreed to provide such Private Information.

176. If Plaintiff and Class Members had known NSC would hand over the PII to a third party with inadequate data security, they would not have agreed to provide such Private Information.

177. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefits of their wrongful conduct.

178. Plaintiff and the Class are without an adequate remedy at law.

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

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

COUNT V
DECLARATORY JUDGMENT
(Alleged Against Both Defendants)
(On behalf of Plaintiff and the Nationwide Class)

181. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

182. Additionally and alternatively, an actual controversy has arisen and exists between Plaintiff and Class Members, on the one hand, and Defendants on the other hand, concerning the Data Breach and Defendants' failure to protect the PII of Plaintiff and the Class Members, and whether Defendants took adequate measures to protect that information. Under the circumstances described herein, Plaintiff and the Class are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations imposed on them by applicable federal and state laws and regulations, industry standards, or otherwise to protect Plaintiff's and Class Members' PII from unauthorized access, disclosure, and use.

183. In view of the ongoing relationships between the parties, and the possession by Defendants of PII belonging to Plaintiff and the Class, a judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they adequately protect PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the

Class, and so that there is clarity between the parties as to Defendant's data security obligations with respect to PII going forward.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

A. An order certifying this action as a Class action, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

B. Judgment in favor of Plaintiff and Class Members awarding them appropriate declaratory relief;

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

D. An order providing declaratory relief as requested herein;

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: November 3, 2023

/s/ Charles L. Williams
Charles L. Williams (VSB No. 23587)
WILLIAMS & SKILLING, P.C.
7104 Mechanicsville Turnpike, Suite 204
Mechanicsville, VA 23111
Telephone: (804) 447-0307, ext. 305
Facsimile: (804) 447-0367
Email: cwilliams@williamsandskilling.com

Jennifer S. Czeisler (*pro hac vice* to be filed)
Edward Ciolko (*pro hac vice* to be filed)
STERLINGTON PLLC
One World Trade Center, 85th Floor
New York, NY 10007
Telephone: (212) 433-2993
Email: Jen.czeisler@sterlingtonlaw.com

Gary F. Lynch (*pro hac vice* to be filed)
Nicholas A. Colella (*pro hac vice* to be filed)
LYNCH CARPENTER LLP
1133 Penn Ave. 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 321-0246
Email: gary@lcllp.com
nick@lcllp.com

Attorneys for Plaintiff

ClassAction.org