Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

IN RE LANSING COMMUNITY COLLEGE DATA BREACH LITIGATION	Master File No. 1:23-cv-00738-PLM Hon. Paul L. Maloney CONSOLIDATED ACTION

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs, Ivory Whitby, Sameer Shah, Gabriel Banish, William Barber, Lindsay Luoma, and Chelsea Lee Ouimette ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Lansing Community College ("LCC" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Complaint against LCC for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: full names and Social Security numbers (collectively, "personally identifiable information" or "PII").

2. Defendant is "one of the largest community colleges in Michigan, serving more than 14,500 students each year."[1]

3. Upon information and belief, former and current students, employees, and applicants for admission or employment are required to entrust Defendant with an extensive amount of their PII, used for Defendant's business, in order to enroll at LCC or be eligible for

[1] https://www.lcc.edu/about/ (last accessed Sept. 15, 2023).

employment. Defendant retains this information for many years after the student and/or employment relationship has ended.

4. "On or around March 14, 2023," Defendant "became aware of suspicious activity on [its] computer network."[2]

5. In response, Lansing Community College "shut itself down on Wednesday [March 15, 2023] because of what it described as an 'ongoing cybersecurity incident.' Lansing Community College suspended nearly all classes and all activities for the rest of the week and asked students and most employees not to work or log into the college's systems or come to campus, according to a message posted on social media."[3] Further, "[m]ost classes were canceled" for the rest of the week, "for Thursday and Friday" as well.[4] The school shutdown disrupted the academic year, including condensing the period during which students took their final exams.

6. At the time, though acknowledging that it lacked certainty, Lansing Community College stated that "it had no evidence that employee or student information has been compromised."[5]

7. In response to the cybersecurity event, Defendant purports to have "immediately launched an investigation, with the assistance of third-party computer specialists."[6] As a result of that investigation, Defendant concluded—on or about May 24, 2023—that "an unauthorized

---

[2] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/9da7ece2-89a4-435a-916d-3ab465e03645.shtml (last accessed Sept. 15, 2023).
[3] https://www.lansingstatejournal.com/story/news/local/2023/03/15/lansing-community-college-suspends-classes-cybersecurity-incident-fbi/70014172007/ (last accessed Sept. 15, 2023).
[4] *Id.*
[5] *Id.*
[6] *See* n.2.

actor may have had access to certain systems" between "December 25, 2022 and March 15, 2023"[7]—this event hereinafter described as the Data Breach.

8. Despite initially announcing no employee or student information was compromised in the Data Breach, Defendant later revealed that PII was indeed compromised in the Data Breach, including that of Plaintiffs. Altogether, the PII of approximately 757,832 individuals (the Class) was compromised.[8]

9. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

10. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect Class Members' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

11. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts

---

[7] *Id.*

[8] According to the report submitted to the Office of the Maine Attorney General, 757,832 individuals were impacted. *See* n.2.

to negligence, at a minimum, and violates federal and state statutes.

12. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

13. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs 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 Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

14. Plaintiffs and Class Members have a continuing interest in ensuring that their PII is and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

PARTIES

15. Plaintiff **Ivory Whitby** ("Plaintiff Whitby") is a natural person, resident, and a citizen of Lansing, Michigan. Defendant obtained and continues to maintain Plaintiff Whitby's PII, and Defendant owed her a legal duty and obligation to protect her PII from unauthorized access and disclosure. Plaintiff Whitby would not have entrusted her PII to Defendant had she

known that Defendant failed to maintain adequate data security. Plaintiff Whitby's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

16. Plaintiff **Sameer Shah** ("Plaintiff Shah") is a natural person, resident, and a citizen of Lansing, Michigan. Defendant obtained and continues to maintain Plaintiff Shah's PII, and Defendant owed him a legal duty and obligation to protect his PII from unauthorized access and disclosure. Plaintiff Shah would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff Shah's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

17. Plaintiff **Gabriel Banish** ("Plaintiff Banish") is a natural person, resident, and a citizen of East Lansing, Michigan. Defendant obtained and continues to maintain Plaintiff Banish's PII, and Defendant owed him a legal duty and obligation to protect his PII from unauthorized access and disclosure. Plaintiff Banish would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff Banish's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

18. Plaintiff **William Barber** ("Plaintiff Barber") is a natural person, resident, and a citizen of East Lansing, Michigan. Defendant obtained and continues to maintain Plaintiff Barber's PII, and Defendant owed him a legal duty and obligation to protect his PII from unauthorized access and disclosure. Plaintiff Barber would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff Barber's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

19. Plaintiff **Lindsay Luoma** ("Plaintiff Luoma") is a natural person, resident, and a citizen of Howell, Michigan. Defendant obtained and continues to maintain Plaintiff Luoma's PII, and Defendant owed her a legal duty and obligation to protect her PII from unauthorized access and disclosure. Plaintiff Luoma would not have entrusted her PII to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Luoma's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

20. Plaintiff **Chelsea Lee Ouimette** ("Plaintiff Ouimette") is a natural person, resident, and a citizen of Waynesville, Missouri. Defendant obtained and continues to maintain Plaintiff Ouimette's PII, and Defendant owed her a legal duty and obligation to protect her PII from unauthorized access and disclosure. Plaintiff Ouimette would not have entrusted her PII to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Ouimette's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

21. Defendant **LCC** is a Michigan-based community college with its principal place of business located at 411 North Grand Avenue, Lansing, Michigan 48933.

JURISDICTION AND VENUE

22. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant,[9] there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

[9] According to the report submitted to the Office of the Maine Attorney General, 138 Maine residents were impacted in the Data Breach. *See id.*

23. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in this District, regularly conducts business in Michigan, and has sufficient minimum contacts in Michigan. Defendant intentionally availed itself of this jurisdiction by marketing and selling its services from Michigan to many businesses nationwide.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

25. Defendant is "one of the largest community colleges in Michigan, serving more than 14,500 students each year."[10]

26. Plaintiffs and Class Members are or were students and/or student applicants at LCC or provided Defendant with their PII for some other purpose (e.g., employment, application for employment, or study).

27. To enroll in classes or other programs at LCC, Plaintiffs and Class Members were required to provide sensitive and confidential PII, including but not limited to: their names and Social Security numbers. The same or similar information was provided by other victims of this Data Breach, including employees of Defendant, applicants for employment, or applicants for admission.

28. Upon information and belief, Defendant made promises and representations to its students, employees, and applicants, including Plaintiffs and Class Members, that the PII collected from them as a condition of their potential or actual enrollment, or potential or actual

[10] *See* n.1.

employment, would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

29. Indeed, the Privacy Statement posted on Defendant's website provides that: "LCC uses appropriate technical and organizational security measures to protect your information when you transmit it to the College and when the College stores it on its information technology systems."[11]

30. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

31. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

32. Defendant had obligations created by the FTC Act, contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

33. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach

34. "On or around March 14, 2023," Defendant "became aware of suspicious activity

[11] https://www.lcc.edu/privacy/index.html (last visited Sept. 15, 2023).

on [its] computer network."[12]

35. In response, Lansing Community College "shut itself down on Wednesday [March 15, 2023] because of what it described as an 'ongoing cybersecurity incident.' Lansing Community College suspended nearly all classes and all activities for the rest of the week and asked students and most employees not to work or log into the college's systems or come to campus, according to a message posted on social media." Further, "[m]ost classes were canceled" for the rest of the week, "for Thursday and Friday" as well.[13]

36. At the time, though acknowledging that it lacked certainty, Lansing Community College stated that "it had ***no*** evidence that employee or student information has been compromised." (Emphasis added).[14]

37. As a result of the campus-wide shutdown, certain classes were cancelled including a disruption and compression of student exam schedules.

38. Following the initial suspected data breach in the middle of March 2023, students were not further informed of the results of the Data Breach, including whether they should safeguard their information, until over three months follow later. On or about June 30, 2023, Defendant began sending Plaintiffs and other victims of the Data Breach a letter titled Notice of Security Incident (the "Notice Letter") informing them that:

> **What Happened?** On or around March 14, 2023, LCC became aware of suspicious activity on our computer network. LCC immediately launched an investigation, with the assistance of third-party computer specialists. Through our investigation, we determined that, between December 25, 2022 and March 15, 2023, an unauthorized actor may have had access to certain systems. In an abundance of caution, LCC reviewed the information on those systems to confirm what information is contained within, and to whom it relates. This process was completed on May 24, 2023. We are

[12] *See* n.2.
[13] *See* n.3.
[14] *Id.*

> notifying you because information related to you was present on the impacted systems.
>
> **What Information Was Involved**? Our investigation determined the following types of your information may have been impacted by this incident: your name and Social Security number.[15]

39. Omitted from the Notice Letter were any explanation as to why Defendant did not detect the Data Breach for *nearly three months* after the breach began, any explanation as to why it took Defendant *over three months* to inform victims of the Data Breach's occurrence after Defendant detected the cyberattack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

40. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

41. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members. causing the exposure of their PII.

42. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and Class Members, including their names and Social Security numbers. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

43. Plaintiffs further believe their PII, and that of Class Members, was subsequently

[15] *See* Exhibit A, Sample Notice Letter (letter to Chelsea L. Fox, a/k/a Plaintiff Chelsea L. Ouimette).

sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

44. Defendant did not use reasonable security procedures and practices, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of the sensitive information they were maintaining for Plaintiffs and Class Members.

45. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[16]

46. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

[16] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Sept. 15, 2023).

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[17]

47. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets
- Apply latest security updates;
- Use threat and vulnerability management;
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise;

[17] *Id.* at 3–4.

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
- Apply principle of least-privilege;

Monitor for adversarial activities

- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[18]

48. Given that Defendant was storing the PII of its current and former students, employees, student applicants, and employee applicants, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

49. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over seven hundred thousand individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' PII

50. Defendant has historically acquired, collected, and stored the PII of Plaintiffs and Class Members.

[18] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Sept. 15, 2023).

51. As a condition to enroll, apply for enrollment, or obtain employment at LCC, Plaintiffs and Class Members are required to give their sensitive and confidential PII to Defendant. Defendant retains this information even after the relationship has ended and Defendant is no longer required to retain this information.

52. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

53. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

54. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

55. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk Because Educational Providers in Possession of PII Are Particularly Susceptible to Cyber Attacks

56. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendant, preceding the date of the Breach.

57. Data breaches, including those perpetrated against educational institutions that

store PII in their systems, have become widespread.[19] Educational institutions are prime targets for cyberattacks because of the type and amount of personal data maintained in their systems.

58. In 2021, a record 1,862 data breaches occurred, affecting approximately 293,927,708 victims who had their sensitive records, a 68% increase from 2020.[20]

59. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[21]

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

61. Defendant knew and understood unprotected or exposed PII in the custody of educational institutions, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

---

[19] *See* https://www.k12dive.com/news/2021-record-year-education-data-breaches/647204/ (last accessed Sept. 15, 2023); https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Parent%20Guide%20to%20Data%20Breach.pdf (last accessed Sept. 15, 2023).

[20] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf (last accessed Sept. 15, 2023)), at 6.

[21] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

62. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

63. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially hundreds of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

65. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

66. That Defendant is encouraging its current and former students and other personnel to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals are subject to a substantial and imminent threat of fraud and identity theft.

67. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

68. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

69. As an educational provider in custody of students', employees', and employee applicants' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] The FTC defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[23]

71. The PII of individuals remains of high value to criminals, as evidenced by the

[22] 17 C.F.R. § 248.201 (2013).
[23] *Id.*

prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[24] For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[25] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[26]

72. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

73. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show

---

[24] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 15, 2023).

[25] *See id.*; *see also Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Sept. 15, 2023).

[26] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sept. 15, 2023).

[27] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 15, 2023).

evidence of actual, ongoing fraud activity to obtain a new number.

74. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, and date of birth.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[29]

77. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

78. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability

---

[28] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Sept. 15, 2023).

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 15, 2023).

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. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

Defendant Fails to Comply with FTC Guidelines

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

80. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[31]

81. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[32]

---

[30] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 15, 2023).
[31] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 15, 2023).
[32] *Id.*

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

83. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. These FTC enforcement actions include actions against higher educational institutions.

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

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

87. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its students, employees, and other personnel. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

88. As noted above, experts studying cyber security characterize entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they

collect and maintain.

89. Several best practices have been identified that at a minimum should be implemented by educational institutions in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backing up data; and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

90. Other best cybersecurity practices that are standard in the higher education industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

92. These foregoing frameworks are existing and applicable industry standards in the higher education industry, and upon information and belief, Defendant failed to comply with at

least one—or all—of these accepted standards, thereby opening the door to the threat of bad actors and causing the Data Breach.

Common Injuries & Damages

93. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Plaintiffs' and Class Member's Risk of Identity Theft

94. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

95. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. Because a person's identity is akin to a puzzle with multiple data points, 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 track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

98. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

99. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

100. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

101. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as checking their financial accounts for any indication

of fraudulent activity, which may take years to detect.

102. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[33]

103. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach 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.

104. And for those Class Members who experience actual identity theft and fraud, as noted *supra*, these victims face "substantial costs and time to repair the damage to their good name and credit record."[34]

Diminution of Value of PII

105. PII is a valuable property right.[35] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[33] *See* n.30.
[34] *See* n.30.
[35] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *1-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

106. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[36]

107. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[37]

108. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a dat a broker who in turn aggregates the information and provides it to marketers or app developers.[38] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[39]

109. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and compounded with the rarity of this data, thereby causes additional loss of value.

110. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to

---

[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sept. 15, 2023).

[37] *See* David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, Los Angeles Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Sept. 15, 2023).

[38] *See, e.g.*, https://datacoup.com/ (last visited Sept. 15, 2023).

[39] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Sept. 15, 2023).

change, e.g., Social Security numbers and names.

111. The fraudulent activity resulting from the Data Breach may not come to light for years.

112. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

113. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

114. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially hundreds of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

115. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable & Necessary

116. Given the type of targeted attack in this case, the sophisticated criminal activity, and the type of PII involved in this Data Breach, there is a strong probability that entire batches of stolen information have been, or will be, placed on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—e.g., opening bank

accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

118. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[40] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

119. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

120. The retail cost of credit monitoring and identity theft monitoring can be around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft arising from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

[40] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Sept. 15, 2023).

Loss of Benefit of the Bargain

121. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services or accepting employment from Defendant under certain terms, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value or were paid less than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Ivory Whitby

122. Although never enrolled, Plaintiff Ivory Whitby applied for admission to LCC in or about 2019.

123. In order to apply for admission, she was required to provide her PII to Defendant.

124. At the time of the Data Breach—December 25, 2022 through March 15, 2023—Defendant retained Plaintiff Whitby's PII in its system.

125. Plaintiff Whitby is very careful about sharing her sensitive PII. Plaintiff Whitby stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

126. Plaintiff Whitby received the Notice Letter, by U.S. mail, directly from Defendant, dated June 30, 2023. According to the Notice Letter, Plaintiff Whitby's PII was improperly accessed and obtained by unauthorized third parties, including her full name and Social Security number.

127. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Whitby made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to, researching the Data Breach to obtain more detailed information on its occurrence and checking their financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Whitby has spent significant time dealing with the Data Breach, valuable time Plaintiff Whitby otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

128. Plaintiff Whitby suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of her PII; and (e) the continued risk to her PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

129. The Data Breach has caused Plaintiff Whitby to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

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

131. Plaintiff Whitby has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

Plaintiff Sameer Shah

132. On or around July 10, 2023, Plaintiff Shah received a Notice Letter from Lansing Community College dated June 30, 2023, informing him that his personal information, including his name and Social Security Number was subject to unauthorized access during the Data Breach.

133. Plaintiff Shah entrusted his PII to Defendant to attend college classes at LCC and/or to receive financial aid, with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

134. The Data Breach caused Plaintiff Shah to lose access to his online courses through LCC for days due to the Data Breach.

135. Plaintiff Shah has been careful to protect and monitor his identity.

136. As a result of the Data Breach, Plaintiff Shah has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Shah has spent time researching the facts and scope of the Data Breach, monitoring his accounts and personal information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Shah received from Lansing Community College specifically directed him to take these actions.

137. Plaintiff Shah plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

138. Plaintiff Shah has also suffered emotional distress resulting from the public release of his PII.

Plaintiff Gabriel Banish

139. Plaintiff Gabriel Banish was a student at LCC. He gave his PII to LCC as a condition of his enrollment.

140. At the time of the Data Breach—December 25, 2022 through March 15, 2023—Defendant retained Plaintiff Banish's PII in its system.

141. Plaintiff Banish is very careful about sharing his sensitive PII. Plaintiff Banish stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

142. Plaintiff Banish was notified that his PII was compromised in the Data Breach.

143. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Banish has spent approximately 1-2 hours monitoring his accounts for incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent monitoring his accounts as a result of the Data Breach is time Plaintiff Banish otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Banish lost was spent at Defendant's direction. Indeed, in the Notice Letter Defendant sent, Defendant directed Plaintiff Banish to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

144. Plaintiff Banish also signed up for credit monitoring through Experian as a result of the Data Breach. Plaintiff Banish plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

145. Plaintiff Banish has also suffered emotional distress from the public release of his

PII. Plaintiff Banish also suffered heightened anxiety and stress from the educational disruption that the Data Breach caused, due to the fact that LCC shut the school down for a week, which impacted his exam schedule and Plaintiff Banish's ability to adequately prepare for his exams.

Plaintiff William Barber

146. Plaintiff William Barber was a student at LCC during the period of August 2021 through August 2023, including at the time of the Data Breach. Plaintiff Barber gave his PII to LCC as a condition of his enrollment.

147. At the time of the Data Breach—December 25, 2022 through March 15, 2023—Defendant retained Plaintiff Barber's PII in its system.

148. Plaintiff Barber is very careful about sharing his sensitive PII. Plaintiff Barber stores any documents containing his PII in a safe and secure location. Plaintiff Barber has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

149. Plaintiff Barber was notified that his PII was compromised in the Data Breach.

150. Subsequent to the Data Breach, Plaintiff Barber, in an effort to mitigate the expected losses here, purchased credit and fraud monitoring through Discover, including Fraud & Security Protections, identity monitoring, and online privacy protection at a cost $15.00 per month.

151. Plaintiff Barber has spent approximately three hours so far taking steps, including monitoring his credit and financial details, to protect himself against any deleterious effects as a result of the Data Breach. The time spent addressing the issues stemming from the Data Breach is time Plaintiff Barber otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Barber lost was spent at Defendant's direction. Indeed, in the Notice Letter Defendant sent, Defendant directed Plaintiff Barber to spend time mitigating

his losses by reviewing his accounts and credit reports for unauthorized activity.

152. Plaintiff Barber plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

153. Plaintiff Barber has also suffered emotional distress from the public release of his PII and anxiety regarding the potential harm from this release.

Plaintiff Lindsay Luoma

154. Plaintiff Lindsay Luoma was a former student and employee at LCC during the period of 2005-2017. She gave her PII to LCC as a condition of her enrollment and employment.

155. At the time of the Data Breach—December 25, 2022, through March 15, 2023—Defendant retained Plaintiff Luoma's PII in its system.

156. Plaintiff Luoma is very careful about sharing her sensitive PII. Plaintiff Luoma stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

157. Plaintiff Luoma was notified that her PII was compromised in the Data Breach.

158. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Luoma experienced actual fraud. On or around March 22, an unauthorized individual filed a tax return in Plaintiff Luoma's name with the IRS. Plaintiff Luoma had to contact the IRS to report and dispute the fraudulent tax return, and had to do a credit check and put holds on her credit report so that nothing could be pulled without her approval. Plaintiff Luoma spent several days communicating with the IRS and otherwise placing holds on her accounts as a result of this fraudulent activity. When she filed her taxes after this incident, she paid approximately $30.00 in postage to ensure that her tax return was received by the IRS. She spent additional time

monitoring her accounts for incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent addressing the instance of tax fraud and monitoring her accounts as a result of the Data Breach is time Plaintiff Luoma otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Luoma lost time was spent at Defendant's direction. Indeed, in the Notice Letter Defendant sent, Defendant directed Plaintiff Luoma to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

159. Plaintiff Luoma plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

160. Plaintiff Luoma has also suffered emotional distress from the public release of her PII.

Plaintiff Chelsea Lee Ouimette

161. Plaintiff Chelsea Lee Ouimette is a former student of LCC, and attended LCC from 2007 through 2011. Plaintiff Ouimette gave her PII to LCC as a condition of her enrollment.

162. At the time of the Data Breach—December 25, 2022, through March 15, 2023—Defendant retained Plaintiff Ouimette's PII in its system.

163. Plaintiff Ouimette is very careful about sharing her sensitive PII. Plaintiff Ouimette stores any documents containing her PII in a safe and secure location. Plaintiff Ouimette has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

164. Plaintiff Ouimette was notified that her PII was compromised in the Data Breach.

165. Following the Data Breach, in 2023, Plaintiff Ouimette experienced actual misuse

of her PII, attempted identity theft, and fraud.

166. Specifically, following the Data Breach, Plaintiff Ouimette experienced, *inter alia*:

a) several unauthorized hard inquiries on her credit reports;

b) several unauthorized fraudulent charges to her debit card, requiring her to obtain a replacement debit card;

c) unauthorized fraudulent charges to her credit cards;

d) identity theft in that an identity thief attempted to obtain a car loan in her name;

e) an increase in the number of unsolicited spam emails and texts.

167. Due to the actual misuse of her PII after the Data Breach, Plaintiff Ouimette was forced to place a fraud alert on her credit, file a police report, and file a report with the Federal Trade Commission.

168. Plaintiff Ouimette has spent a significant amount of time monitoring her accounts for additional incidents of identity theft and fraud as a result of the Data Breach. The time spent addressing the instance of tax fraud and monitoring her accounts as a result of the Data Breach is time Plaintiff Ouimette otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Ouimette lost was spent at Defendant's direction. Indeed, in the Notice Letter Defendant sent, Defendant directed Plaintiff Ouimette to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

169. Altogether, Plaintiff Ouimette estimates that she has spent approximately 84 hours to date taking steps to mitigate the effects of the above-described fraudulent activity.

170. Plaintiff Ouimette plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

171. Plaintiff Ouimette has also suffered emotional distress from the public release of her PII and anxiety resulting from the already present harm and additional harm likely she is likely to suffer.

172. Plaintiff Ouimette has also suffered severe emotional distress and anxiety due to the fact that her husband's employment is conditioned upon maintaining his security clearance and the fraudulent activity suffered here makes it harder to maintain his security clearance. She fears her husband may lose his job due to the Data Breach and the fraud she has experienced.

173. Plaintiff Ouimette has also suffered severe emotional distress due to the amount of time that she has had to spend handling the fraudulent activity rather than spending time with her family and her children.

CLASS ACTION ALLEGATIONS

174. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

175. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose PII was compromised as a result of the Data Breach, for which Defendant provided notice in June 2023 (the "Class").

176. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

177. Plaintiffs hereby reserve the right to amend or modify the Class definitions with greater specificity or division after having had an opportunity to conduct discovery. The

proposed Class meets the criteria for certification.

178. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. At least 757,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine's Attorney General's Office.[41] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. 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;

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

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

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

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

[41] *See* n.2.

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant was unjustly enriched;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

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

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

183. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution

of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of 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.

184. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

186. And all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST COUNT
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

187. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

188. Plaintiffs and Class Members entered into valid and enforceable contracts through which they were required to turn over their PII to LCC in exchange for services and/or employment. That contract included promises by LCC to secure, safeguard, and not disclose Plaintiffs' and Class Members' PII to any third parties without their consent.

189. CMS's Privacy Statement memorialized the rights and obligations of LCC and its students and/or employees. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services and/or employment at LCC.

190. In its Privacy Statement, LCC commits to protecting the privacy and security of the PII and promises to never share Plaintiffs' and Class Members' PII except under certain limited circumstances.

191. Plaintiffs and Class Members fully performed their obligations under their contracts with LCC. However, LCC failed to secure, safeguard, and/or keep private Plaintiffs' and Class Members' PII, and, therefore, LCC breached its contracts with Plaintiffs and Class Members.

192. LCC's failure to satisfy its confidentiality and privacy obligations resulted in LCC providing services and/or employment to Plaintiffs and Class Members that were of a diminished value and in breach of its contractual obligations to Plaintiffs and Class Members.

193. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including by LCC's failure to fully perform its part of the agreement

with Plaintiffs and Class Members.

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

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

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

196. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

197. When Plaintiffs and Class Members provided their PII to Defendant in exchange for enrolling in classes, applying for enrollment, or obtaining employment at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any PII that it was no longer required to maintain.

198. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

199. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

200. In accepting the PII of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard their PII from unauthorized access or disclosure.

201. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTC Act, Michigan statutes, and were consistent with industry standards.

202. Plaintiffs and Class Members paid money and/or provided their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

203. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

204. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of Defendant's implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

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

206. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their PII or to destroy it once it was no longer necessary to retain the PII.

207. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

208. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach and Defendant's breach of the implied

contracts.

209. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Plaintiffs and Class Members.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

210. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

211. This count is pleaded in the alternative to the Breach of Express Contract claim (Count I) and Breach of Implied Contract claim (Count II) above.

212. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class Members, and/or revenue generated as a direct result of employment.

213. As such, a portion of the payments made by or on behalf of, and/or revenue generated by, Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made, and/or revenue generated as a direct result of employment, that is allocated to data security is known to Defendant.

214. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII and paid money to Defendant in connection with their admission applications and/or provided their labor to Defendant and/or its agents, and in so doing, provided Defendant with their PII based on the understanding that the benefits derived therefrom would, in part, be used to fund adequate data security. In exchange, Plaintiffs and Class Members

should have received from Defendant the goods, services, and/or employment that were the subject of the transaction and their PII should have been protected with adequate data security.

215. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

216. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and instead directed those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

217. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

218. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

219. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

220. Defendant obtained a benefit from Plaintiffs and Class Members by fraud and/or the taking of an undue advantage, in that it misrepresented and omitted material information concerning its data security practices when Plaintiffs and Class Members relied upon it to

safeguard their PII against foreseeable risks.

221. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

222. Plaintiffs and Class Members have no adequate remedy at law.

223. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

224. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injuries and/or harms.

225. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and

Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to customer and employee data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

1. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

2. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

3. Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

4. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

5. Prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

7. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

8. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

9. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

10. Requiring Defendant to conduct regular database scanning and securing checks;

11. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

12. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

13. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

14. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

15. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

16. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

17. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final

judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: September 15, 2023

Respectfully submitted,

/s/ Benjamin F. Johns

Jonathan Shub
Benjamin F. Johns
Samantha E. Holbrook
SHUB & JOHNS LLC
Four Tower Bridge,
200 Barr Harbor Drive, Ste
400 Conshohocken, PA 19428
T: (610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com

sholbrook@shublawyers.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Nick Suciu
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301
Tel: (313) 303-3472
Email: nsuciu@milberg.com

E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

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

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

**pro hac vice to be filed*

Attorneys for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on September 15, 2023, I electronically filed the foregoing document(s) using the Court's electronic filing system, which will notify all counsel of record authorized to receive such filings.

Dated: September 15, 2023

Respectfully submitted,

/s/ Benjamin F. Johns
Benjamin F. Johns
SHUB & JOHNS LLC
Four Tower Bridge,
200 Barr Harbor Drive, Ste
400 Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com

Exhibit A

LANSING COMMUNITY COLLEGE

June 30, 2023

[redacted]

NOTICE OF SECURITY INCIDENT

Dear CHELSEA L FOX,

Lansing Community College ("LCC") writes to notify you of an incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around March 14, 2023, LCC became aware of suspicious activity on our computer network. LCC immediately launched an investigation, with the assistance of third-party computer specialists. Through our investigation, we determined that, between December 25, 2022 and March 15, 2023, an unauthorized actor may have had access to certain systems. In an abundance of caution, LCC reviewed the information on those systems to confirm what information is contained within, and to whom it relates. This process was completed on May 24, 2023. We are notifying you because information related to you was present on the impacted systems.

What Information Was Involved? Our investigation determined the following types of your information may have been impacted by this incident: your name and Social Security number. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

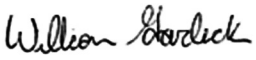
What We Are Doing. Data privacy and security are among LCC's highest priorities, and we have measures in place to help protect information in LCC's care. Upon discovery, LCC promptly commenced an investigation with the assistance of third-party computer specialists to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities, as required by law. In addition, we notified law enforcement and are cooperating with its investigation.

As an added precaution, we are also offering 12 months of complimentary access to identity monitoring services through Kroll. Individuals who wish to receive these services must activate by following the attached activation instructions.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Personal Information.* There you will also find more information on the complimentary credit monitoring services we are making available to you. While LCC will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-547-5959 between the hours of 9:00 a.m. and 6:30 p.m. EST, Monday – Friday, excluding some major U.S. holidays. You may also write to LCC at 411 N. Grand Avenue, Attention: Risk Management - Jean Richard Beauboeuf, Lansing, Michigan 48933.

Sincerely,



Bill Garlick
Chief Information Officer
www.lcc.edu

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **9/26/2023** to activate your identity monitoring services.*

Membership Number: **DYKU28878-P**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;

4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to help protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately fifty-five (55) Rhode Island residents that may be impacted by this event.