UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
HAMMOND DIVISION

ZACHARY CLARK, on behalf of himself, and all others similarly situated,	)	
Plaintiff,	)	
v.	)	Case No. 2:25-cv-451
VALPARAISO UNIVERSITY,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, Zachary Clark ("Plaintiff"), on behalf of himself and all others similarly situated, complains and alleges as follows against Defendant, Valparaiso University ("Defendant" or "Valpo") based on personal knowledge, on the investigation of his counsel, and on information and belief as to all other matters:

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Valpo, arising from its failure to safeguard certain Personally Identifying Information[1] ("PII") and other sensitive, non-public financial information (collectively, "Personal Information") of thousands of its current, former, and prospective students (collectively, "students") and employees, as well as others whose personal information was stored on Valpo's

[1] The Federal Trade Commission defines "personally 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." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the breach.

systems.

2. Valpo's failure to safeguard these individuals' PII resulted in Defendant's network systems being unauthorizedly accessed by hackers and the Personal Information of Plaintiff and other students and employees, being disclosed, stolen, compromised, and misused, causing widespread and continuing injury and damages.

3. On information and belief, between August 7, 2025, and August 8, 2025, Valpo's network was unauthorizedly infiltrated and encrypted, resulting in the unauthorized disclosure of the Personal Information of Plaintiff and the Class Members, including names, Social Security numbers, Driver's License/State Identification number, and/or financial account information (e.g., account number, credit or debit card in combination with security code, password, or access code) (the "Data Breach"). *See* Valpo Notice of Data Breach, September 19, 2025 ("Notice"), a copy of which is attached as **Exhibit A.**[2]

4. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by Valpo, and the resulting monetary damages including out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals as a result of the tortious conduct of Defendant.

5. As a consequence of the Data Breach, Plaintiff and the Proposed Class Members' sensitive Personal Information has been released into the public domain and they have had to, and

[2] *See also*, Valparaiso University, Notice of Data Incident available at: https://www.valpo.edu/notice-of-data-incident/ (last accessed September 26, 2025).

will continue to have to, spend time, effort, and money to protect themselves from fraud and identity theft.

6. Further, and to compound the harm, Defendant waited one (1) month before Defendant publicly disclosed the incident. While the Notice states that Defendant detected the Data Breach by August 11, 2025, Defendant did not post the Notice until September 19, 2025. *Id.*

7. As a result of the Data Breach, Plaintiff and the Proposed Class Members have been required to take measures to deter and detect identity theft and fraud. Plaintiff and the Proposed Class Members have been required to take the time and effort, which they otherwise would have dedicated to other life demands, to mitigate the actual and potential impact of the Data Breach including, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports, financial accounts, explanations of benefits, and medical accounts for unauthorized activity.

8. Defendant disregarded the rights of Plaintiff and the Proposed Class Members by failing to take and implement adequate and reasonable measures to ensure that the Personal Information it stores was safeguarded; failing to take available steps to prevent the Data Breach from happening; failing to follow the mandatory, applicable, and appropriate protocols, policies, and procedures; and failing to timely notify Plaintiff and the Proposed Class Members.

9. As the direct result of Defendant's actions, the Personal Information of Plaintiff and the Proposed Class Members was compromised and stolen by unauthorized third parties.

10. Because this same information remains stored in Defendant' systems, Plaintiff and the Proposed Class members have an interest in ensuring that Defendant takes the appropriate measures to protect their information against future unauthorized disclosures.

11. On behalf of himself and the Class preliminarily defined below, Plaintiff brings causes of action for negligence, negligence *per se*, breach of express and implied contractual duties, unjust enrichment, invasion of privacy, and bailment. Plaintiff seeks damages and injunctive and declaratory relief arising from Valpo's failure to adequately protect his highly sensitive Personal Information.

PARTIES

12. Plaintiff, Zachary Clark, is a natural person, citizen, and resident of Michigan. Plaintiff Clark is among thousands of individuals whose Personal Information was disclosed to unauthorized third parties during the Data Breach.

13. Plaintiff Clark is a former student and graduate of Valpo.

14. Plaintiff Clark paid tuition and fees for educational services provided by the Defendant to the Plaintiff.

15. Plaintiff Clark received a notice from Valpo stating that his Personal Information including his name and Social Security Number, and financial information were compromised during the Data Breach.

16. Defendant, Valparaiso University is a private university located in Valparaiso, Indiana.

JURISDICTION AND VENUE

17. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because: (i) there are more than one hundred (100) Class Members; (ii) the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (iii) some Class Members are citizens of states different than Valpo.

18. This Court has personal jurisdiction over Valpo because it regularly and

systematically transacts business in the State of Indiana, such that it can reasonably anticipate defending a lawsuit here.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and/or a substantial part of property that is the subject of this action is situated herein.

FACTUAL ALLEGATIONS

A. Plaintiff and the Class Members entrusted their Personal Information to Valpo

20. Defendant, Valpo, is a private, Lutheran-affiliated university in Valparaiso, Indiana.

21. In the ordinary course of providing educational services, students are required to provide Defendant with sensitive, personal, and private information such as their name, address, phone number and email address; date of birth; demographic information; social security number; photo identification; employer information; financial account information; driver's license or state identification number; and other information that may be deemed necessary by the Defendant. Similarly, Valpo employees are required to provide Valpo with Personal Information as a condition of employment.

22. Valpo acquired, collected, and stored a massive amount of said Personal Information of its students, employees, and others, including Plaintiff= and the Members of the proposed Class, which it stored in its electronic systems.

23. By obtaining, collecting, using, and deriving a benefit from its students' and employees' Personal Information, Valpo assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Personal Information from unauthorized disclosure.

24. Plaintiff has taken reasonable steps to maintain the confidentiality of his Personal Information. Plaintiff and the Class Members, as individuals who were required to entrusted their Personal Information to Valpo, relied on Valpo to keep their Personal Information confidential and securely maintained, and to use their information for authorized purposes and disclosures only.

25. In addition, Valpo maintains a Copyright and Privacy Policy (the "Privacy Policy")[3] on its website, where it acknowledges its obligations to safeguard Personal Information:

> Any information collected from visitors to our website, including demographics, Internet Protocol addresses, Domain Name Server information, and e-mail addresses, will be used solely for internal informational purposes by Valparaiso University and will not be given, sold, or otherwise redistributed to any unauthorized third party. Ex. B at 1.

Id.

26. Plaintiff and the proposed Class Members entrusted their Personal Information to Valpo with the expectation and implied mutual understanding that Valpo would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

27. Plaintiff and the proposed Class Members would not have entrusted Valpo with their highly sensitive Personal Information if they had known that Valpo would fail to take adequate measures to protect it from unauthorized use or disclosure.

B. Plaintiff and the Class Members' Personal Information was Unauthorizedly Disclosed and Compromised in the Data Breach

28. Plaintiff Clark was a student at Valpo and graduated from Valpo in 2014.

29. As a prerequisite to enrollment, Plaintiff and the Class Members disclosed their

[3] *See* **Exhibit B**, also available at https://www.valpo.edu/copyright-and-privacy-policy/ (last accessed Sept. 26, 2025).

non-public and sensitive Personal Information to Valpo, with the implicit understanding that their Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their enrollment there, and the express, specific, written representations made by Valpo and its agents.

30. Plaintiff and the Class Members reasonably relied upon Valpo's representations to their detriment and would not have provided their sensitive Personal Information to Valpo if not for Valpo's explicit and implicit promises to adequately safeguard that information.

31. On or about September 19, 2025, Valpo posted a Notice of Data Incident on its website providing notification that Personal Information had been compromised during the Data Breach and they began working with third-party specialists to investigate. Potentially impacted victims are still being notified.

32. According to Valpo's Notice of Data Incident, "On August 11, 2025, our investigation determined that certain files and folders were copied and/or downloaded by an unknown third party between August 7, 2025, and August 8, 2025. Although the review remains ongoing, the type of information potentially impacted likely varies by individual but may include name and one or more of the following: Social Security number, driver's license or state identification number, and/or financial account information." *Id*.

33. Valpo is in the process of conducting a comprehensive review of the relevant files and folders to determine the full nature and scope of the information at risk. Valpo encourages those affected by the Data Breach "to remain vigilant against incidents of identity theft and fraud by reviewing credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors." *Id*. Valpo also provided other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your

credit files, and/or obtaining a free credit report. *Id*.

34. Despite Valpo claiming in its Notice that the data breach may impact certain individuals, they state that individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax.

35. As a result of this Data Breach, the Personal Information of Plaintiff and the proposed Class Members, was unauthorizedly disclosed and compromised in the Data Breach.

36. The Data Breach was preventable and a direct result of Valpo's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Personal Information.

37. In addition, Valpo alleges it discovered the Data Breach on August 11, 2025, an investigation was instituted, and steps were taken to ensure the security of their computer systems, notify law enforcement, and are providing notification to the potentially impacted individuals. Therefore, the scope of the breach and its affected victims are still unknown.

C. Valpo Failed to Sufficiently Protect the Personal Information that Plaintiff and the Proposed Class Members Had Entrusted to It.

38. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[4] The next year, that number increased by nearly 50%.[5]

39. The Personal Information stolen in the Data Breach is significantly more valuable

---

[4] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/.

[5] *2017 Annual Data Breach Year-End Review*, ITRC, (Jan. 25, 2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach— most notably names and Social Security Numbers—is difficult, if not impossible, to change.

40. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[6]

41. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining PII with false provider numbers to file fake claims with insurers.

42. The value of Plaintiff' PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

43. Email phishing schemes "remain[] the primary attack vector for nine out of 10 cyberattacks."[7] Valpo did not elaborate on how the Data Breach happened, other than that an unauthorized third party infiltrated its network and certain files and folders were copied and/or

---

[6] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[7] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH, (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

downloaded.

44. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

45. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PII.

46. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

i. Valpo failed to adhere to FTC guidelines

47. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[8] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Valpo, should employ to protect against the unlawful exposure of Personal Information.

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*

[8] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

for Business, which established guidelines for fundamental data security principles and practices for business.[9] The guidelines explain that businesses should:

a. protect the personal information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

49. The FTC 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.[10]

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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.

---

[9] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[10] *See Start with Security*, *supra* n.40.

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

52. Valpo failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining and communicating sensitive data.

53. Valpo's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

ii. Valpo failed to adhere to GLBA guidelines

54. The Federal Trade Commission considers Title IV-eligible institutions, like Valpo, that participate in Title IV Educational Assistance Programs as "financial institutions" and subject to the Gramm-Leach-Bliley Act (16 CFR 313.3(k)(2)(vi)) ("GLBA").

55. The GLBA's Safeguard Rule requires the following in relevant parts:

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

. . . (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

. . . (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material

> changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

56. The GLBA creates a duty for Defendant to safeguard Plaintiff's and the Class Members' Personal Information.

57. Defendant was obligated by federal law, its own policies, and industry standards to keep Plaintiff's and Class Members' Personal Information entrusted to Defendant confidential and to protect it from unauthorized access and disclosure.

58. However, Defendant has failed to adequately implement such policies. This failure to implement has resulted in the Data Breach at issue.

59. Defendant's policies and procedures to safeguard the Personal Information of the Plaintiff and other Proposed Class Members were inadequate, insufficient, and non-compliant with its statutory obligations.

60. Plaintiff and Proposed Class Members provided their Personal Information 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.

61. Plaintiff and Proposed Class Members reasonably believed that Defendant would maintain their Personal Information in a secure manner and relied upon this understanding when providing said information to the Defendant.

62. Had Plaintiff and Proposed Class Members known that Defendant would not maintain their information in a reasonably secure manner, they would not have provided their Personal Information to Defendant.

63. Defendant could have easily prevented this Data Breach. Defendant is aware of the

value of Personal Information and the risks associated with unauthorized disclosure of this information, yet Defendant failed to implement adequate measures to protect its students, employees, and other affiliated individuals' Personal Information.

64. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the Personal Information maintained on its systems. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to implement its promised Privacy Policy;

c. Failing to adhere to FTC and GLBA standards;

d. Failing to adequately protect Proposed Class Members' Personal Information;

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

f. Failing to provide timely notice of the breach.

D. Plaintiff and the Class Members were Significantly Injured by the Data Breach

65. As a result of Valpo's failure to prevent the Data Breach, Plaintiff Clark, along with the Class Members, has suffered and will continue to suffer significant injury and damages. They have suffered or are at increased risk of suffering:

a. Misuse of Personal Information,

b. The loss of the opportunity to control how Plaintiff's and the Class Members' Personal Information is used;

c. The diminution in value of their Personal Information;

d. The compromise, publication and/or theft of their Personal Information;

e. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

f. Increased receipt of spams, calls and texts,

g. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Delay in receipt of tax refund monies;

i. Unauthorized use of stolen Personal Information;

j. The continued risk to their Personal Information, which remains in the possession of Valpo and is subject to further breaches so long as it fails to undertake appropriate measures to protect the Personal Information in their possession; and

k. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

66. As a result of the Data Breach, Plaintiff and the Class Members now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

67. After the breach, Plaintiff Calrk has reported receiving spam texts and phone calls.

68. As a long-standing member of the higher educational community, Valpo knew or should have known the importance of safeguarding Personal Information entrusted to it and of the

foreseeable consequences of a breach. Despite this knowledge, however, Valpo failed to undertake adequate cyber-security measures to prevent the Data Breach email attack from happening.

69. Valpo has encouraged affected victims to review credit reports, account statements, and explanation of benefits forms for suspicious activity or errors. They also state that individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. However, this will not adequately compensate Plaintiff and the Class Members for the injuries and damage resulting from the Data Breach which Defendant failed to prevent.

70. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[11]

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this Class Action on behalf of himself and all others similarly situated pursuant to Fed. R. Civ. Proc. 23. The Class is preliminarily defined as:

> All individuals whose Personal Information was compromised as a result of the Data Breach with Valpo which was announced on or about September 19, 2025.

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

73. Plaintiff reserves the right to modify or amend the definition of the proposed Class

---

[11] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

and/or to add a subclass(es) if necessary, before this Court determines whether certification is appropriate.

74. *Fed. R. Civ. Proc. 23(a)(1) Numerosity:* The Class is so numerous such that joinder of all Members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of thousands of current and former students, employees, and other individuals affiliated with Valpo, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to Valpo's records. Valpo has the administrative capability through its computer systems and other records to identify all Members of the Class, and such specific information is not otherwise available to Plaintiff.

75. *Fed. R. Civ. Proc. 23(a)(2) Commonality and Fed. R. Civ. Proc. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Members of the Class because Valpo has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Valpo had a duty to protect student, employee, and other Valpo-affiliated individuals' Personal Information;

b. Whether Valpo knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Valpo's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether Valpo was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Valpo's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Valpo's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure of the Plaintiff's and Class Members' Personal Information;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Valpo's failure to reasonably protect its systems and data network;

h. Whether Plaintiff and Class Members are entitled to relief;

i. Whether Valpo failed to adequately notify Class Members of the compromise of their Personal Information;

j. Whether Valpo assumed a fiduciary duty and/or confidential relationship to Class Members when they entrusted it with their Personal Information;

k. Whether Valpo breached its contracts with Class Members by failing to properly safeguard their Personal Information and by failing to notify them of the Data Breach;

l. Whether Valpo's violation of FTC and GLBA regulations constitutes evidence of negligence or negligence *per se*;

m. Whether Valpo impliedly warranted to Class Members that the information technology systems were fit for the purpose intended, namely the safe and secure processing of Personal Information, and whether such warranty was breached.

76. *Fed. R. Civ. Proc. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims

of all Class Members, because all such claims arise from the same set of facts regarding Valpo's failures:

a. to protect Plaintiff's and Class Members' Personal Information;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal Information.

77. *Fed. R. Civ. Proc. 23(a)(4) Adequacy:* Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff are victims of the Data Breach, has suffered injury and damages such as misuse and fraudulent activity as a result of the Data Breach, and bring the same claims on behalf of themselves and the putative Class. Plaintiff has no interests antagonistic to that of the Class Members. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

78. *Fed. R. Civ. Proc. 23(b)(2) Injunctive and Declaratory Relief:* Valpo has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

79. *Fed. R. Civ. Proc. 23(b)(3) Superiority:* It is impracticable to bring Class Members' individual claims before the Court. Class treatment permits many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the

unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

80. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

a. The unnamed Members of the Class are unlikely to have an interest in individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is desirable;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

81. Plaintiff know of no unique difficulty to be encountered in the prosecution of this action that would preclude its maintenance as a class action.

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

a. Whether Valpo owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Personal Information;

b. Whether Valpo's security measures to protect its data systems were

reasonable considering best practices recommended by data security experts;

c. Whether Valpo's failure to institute adequate protective security measures amounted to negligence;

d. Whether Valpo failed to take commercially reasonable steps to safeguard students' and employees' Personal Information; and

e. Whether adherence to FTC and GLBA data security recommendations, and industry standards on data security would have reasonably prevented the Data Breach.

83. Finally, all Members of the proposed Class are readily ascertainable. Valpo has access to student, employee and applicant names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

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

84. Plaintiff and the Members of the Class incorporate the above allegations as if fully set forth herein.

85. Defendant Valpo owed a duty to Plaintiff and the Members of the Class to exercise reasonable care to safeguard their Personal Information in its possession, based on the foreseeable risk of a data breach and the resulting exposure of their information, as well as on account of the special relationship between Defendant and its students and employees, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at

unauthorized access.

86. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Members of the Class's Personal Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

87. Further, Defendant owed to Plaintiff and Members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Members of the Class to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

88. Valpo owed these duties to Plaintiff and Members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Members of the Class's personal information and PII for employment purposes.

89. Plaintiff and Members of the Class were required to provide their Personal Information to Defendant as a condition of applying for employment and/or as a condition of employment, and Defendant retained that information.

90. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendant holds vast amounts of this

information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Personal Information, whether by email hacking attack, or otherwise.

91. Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Members of the Class, and the importance of exercising reasonable care in handling it.

92. Defendant Valpo breached its duties by failing to exercise reasonable care in supervising its employees and agents, and in handling and securing the Personal Information and PII of Plaintiff and Members of the Class which actually and proximately caused the Data Breach and Plaintiff's and Members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Members of the Class's injuries-in-fact.

93. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Members of the Class have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

94. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing,

imminent, immediate, and which they continue to face.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Class)

95. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

96. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' Personal Information, PII.

97. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, students' and employees' PII.

98. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

99. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its students' and employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had required and solicited, collected, and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to students and employees in the event of a breach, which ultimately came to pass.

100. The harm that has occurred in the Data Breach is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid

unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

101. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their PII.

102. Defendant breached its respective duties to Plaintiff and Members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' PII.

103. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

104. But for Valpo's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the Members of the Class would not have been injured.

105. The injury and harm suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and Members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

106. Had Plaintiff and Members of the Class known that Defendant did not adequately protect students' and employees' PII, Plaintiff and Members of the Class would not have entrusted Defendant with their PII.

107. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered harm, injury, and damages as set forth in the preceding paragraphs.

COUNT III
BREACH OF EXPRESS/IMPLIED CONTRACTUAL DUTY
(On behalf of Plaintiff and the Class)

108. Plaintiff and Members of the Class incorporate the above allegations as if fully set

forth herein.

109. Defendant offered to provide educational services to Plaintiff and Members of the Class in exchange for payment. Valpo also required Plaintiff and the Members of the Class to provide Defendant with their Personal Information as a condition of applying for educational services.

110. Defendant offered to provide employment to Members of the Class in exchange for labor. Valpo also required Members of the Class to provide Defendant with their Personal Information as a condition of receiving renumeration for labor rendered.

111. In turn, and through its Privacy Policy, Defendant agreed it would not disclose Personal Information it collects to unauthorized persons. Defendant also promised to maintain safeguards to protect their Personal Information.

112. Plaintiff and the Members of the Class accepted Defendant's offer by providing Personal Information to Valpo, in applying for educational services and/or employment, and providing labor to Defendant and receiving renumeration.

113. The agreement was supported by adequate consideration.

114. Implicit in the Parties' agreement was that Defendant would provide Plaintiff and Members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Personal Information.

115. Plaintiff and the Members of the Class would not have entrusted their Personal Information to Defendant in the absence of such agreement with Defendant.

116. Valpo materially breached the contract(s) it had entered with Plaintiff and Members of the Class by failing to safeguard such Personal Information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further

breached the implied contracts with Plaintiff and Members of the Class by:

a. Failing to properly safeguard and protect Plaintiff' and Members of the Class's Personal Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendant received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

117. The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its agreement(s).

118. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

119. The covenant of good faith and fair dealing is implied into every contract. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

120. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

121. Defendant failed to advise Plaintiff and Members of the Class of the Data Breach

promptly and sufficiently.

122. In these and other ways, Defendant violated its duty of good faith and fair dealing.

123. Plaintiff and Members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

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

124. Plaintiff and Members of the Classes incorporate the above allegations as if fully set forth herein.

125. This claim is pleaded in the alternative to the breach of express/implied contractual duty claim.

126. Plaintiff and Members of the Classes conferred a benefit upon Defendant in the form of tuition fees in exchange for educational services or labor rendered in exchange for renumeration.

127. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class. Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the student and employment relationship, as well as for the purpose of applying for enrollment or employment.

128. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the value of their tuition payments or labor with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Classes were entitled to, and that tuition or labor without reasonable data privacy and security practices and procedures that they received.

129. Under principals of equity and good conscience, Defendant should not be permitted to retain the monetary value of the tuition or labor belonging to Plaintiff and Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Classes expended tuition or labor and that were otherwise mandated by federal, state, and local laws and industry standards.

130. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY
(On behalf of Plaintiff and the Class)

131. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

132. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class Members by disclosing and exposing Plaintiff's and the Class Members' Personal Information to enough people that it is reasonably likely those facts have and/or will become known to the public at large, including, without limitation, on the dark web and elsewhere.

133. The disclosure of students' and employees' full names, Social Security numbers, and financial information, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

134. Defendant has a special relationship with Plaintiff and the Class Members and Defendant's disclosure of Personal Information is certain to embarrass them and offend their

dignity. Defendant should appreciate that the cyber-criminals who stole the Personal Information would fraudulently misuse that Personal Information, and further sell and disclose the data, just as they are doing. That the original disclosure is devastating to the Plaintiff and the Class Members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large considering that said non-public information is now made public, and cannot be secured again.

135. The tort of public disclosure of private facts is recognized in Indiana. Plaintiff's and the Class Members' Personal Information was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Class Members' PII is not a matter of legitimate public concern.

136. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages, as set forth herein.

COUNT VI
BAILMENT
(On behalf of Plaintiff and the Class)

137. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

138. Plaintiff, the Class Members, and Defendant contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to Defendants solely for the purpose of obtaining an education and/or employment.

139. Plaintiff and the Class entrusted their PII to Defendant for a specific purpose—for tuition and/or employment—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

140. Defendant accepted the Plaintiff's and the Class's PII for the specific purpose of tuition and/or employment.

141. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and the Class's PII.

142. Plaintiff's and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

143. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Zachary Clark, on behalf of himself and all others similarly situated, respectfully prays this Honorable Court for judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representative and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, hereby demands a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: September 30, 2025

Respectfully submitted,

s/ Lynn A. Toops
Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenmalad.com
athomas@cohenmalad.com

Samuel J. Strauss*
Raina Borrelli*
STRAUSS BORRELLI PLLC
908 N. Michigan Avenue, Suite 1610
Chicago Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

*Motion for *Pro Hac Vice* Admission to be made pursuant to Fed. R. Civ. Proc. 89(b)

Counsel for Plaintiff and the Proposed Class

VALPARAISO UNIVERSITY

← Valpo Stories

Notice of Data Incident

September 19, 2025

Valparaiso University ("Valpo") is providing notification of an event that may impact certain individual. Valpo recently experienced unusual activity on our network. In response, we quickly began working with third-party specialists to conduct an investigation. On August 11, 2025, our investigation determined that certain files and folders were copied and/or downloaded by an unknown third party between August 7, 2025, and August 8, 2025. Valpo is in the process of conducting a comprehensive review of the relevant files and folders to determine the full nature and scope of the information at risk. Although the review remains ongoing, the type of information potentially impacted likely varies by individual but may include name and one or more of the following: Social Security number, driver's license or state identification number, and/or financial account information.

In response to this event, we quickly began an investigation to determine its full nature and scope. We also took steps to ensure the security of our computer systems, notify law enforcement, and are providing notification to the potentially impacted individuals. We are also taking steps to further enhance our cybersecurity posture by reviewing and implementing, as needed, additional policies and procedures, including ensuring the security of data stored on our systems. If you have questions about this incident please call at 1-833-844-9953, Monday through Friday, between 8:00 AM and 8:00 PM ET, excluding holidays. You may also write to us at 1700 Chapel Drive, Valparaiso, IN 46383.

In general, we encourage potentially affected individuals to remain vigilant against incidents of identity theft and fraud by reviewing credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228.

Individuals have the right to place an initial or extended fraud alert on a credit file at no cost. If individuals are a victim of identity theft, they are entitled to an extended fraud alert lasting seven years. As an alternative to a fraud alert, they have the right to place a credit freeze on a credit report. The credit freeze is designed to prevent credit, loans, and services from being approved without consent. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on your credit report.

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

TransUnion Experian Equifax

1-800-680-7289 1-888-397-3742 1-888-298-0045

www.transunion.com www.experian.com www.equifax.com

Individuals can further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps to protect their personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or their state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement, the state Attorney General, and the FTC.

SHARE THIS POST:

PREVIOUS POST

Exploring AI at Valpo: English Professors Light the Path to Future–Ready Skills →

NEXT POST

Recognized for Excellence: How Valparaiso University is Getting National Attention →

Media Contacts

For media inquires, please contact the Office of the President.

OFFICE OF THE PRESIDENT

219.464.5115

Heritage Hall, 510 Freeman Street
Valparaiso University, Valparaiso, IN 46383

Valparaiso, IN 46383-6493 USA

219.464.5000

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

ZACHARY CLARK, on behalf of himself, and all others similarly situated

(b) County of Residence of First Listed Plaintiff Oakland Co., Michigan
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Lynn A. Toops, CohenMalad, LLP, One Indiana Square, Suite 1400, Indianapolis, Indiana 46204, (317) 636-6481

DEFENDANTS

VALPARAISO UNIVERSITY

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C § 1332(d)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
09/30/2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Lynn A. Toops

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Indiana

ZACHARY CLARK, on behalf of himself, and all others similarly situated

Plaintiff(s)

v.

VALPARAISO UNIVERSITY

Defendant(s)

Civil Action No. 2:25-cv-451

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Valparaiso University
c/o Registered Agent, Mark C. Volpatti
1700 Chapel Drive
Valparaiso, Indiana 46383

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Lynn A. Toops
CohenMalad, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: