IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

MATTHEW WILLIAMS, individually and on behalf of all others similarly situated, Plaintiff, v. CARL BUDDIG AND COMPANY, Defendant.	:	CASE NO.: 2024CH09830 CLASS ACTION

CLASS ACTION COMPLAINT

Plaintiff Matthew Williams, ("Plaintiff"), individually and on behalf of all similarly situated individuals, brings this Class Action Complaint against Carl Buddig and Company ("Defendant"), and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. Plaintiff seeks monetary damages and injunctive and declaratory relief in this action, arising from Defendant's failure to safeguard the Personally Identifiable Information ("PII") of Plaintiff and the Class members, including, without limitation: name, social security number, and medical information.

2. Defendant is an Illinois-based meatpacking supplier who employed Plaintiff during 2020.

3. In the course of its business operations, Defendant is entrusted with an extensive amount of Plaintiff's and the Class members' PII.

4. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff and the Class members.

5. In approximately April and May of 2023, an intruder gained entry to Defendant's database, accessed Plaintiff's and the Class members' PII, and exfiltrated information from Defendant's systems (the "Data Breach Incident").

6. Defendant did not notify Plaintiff and the Class members of the incident until at least on year later, April 17, 2024, even though Defendant was aware of suspicious activity by at least May 29, 2023.

7. Plaintiff's and the Class members' PII that was acquired in the Data Breach Incident can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and the Class members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. Plaintiff's and the Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's and the Class members' PII.

9. Until notified of the Data Breach Incident, Plaintiff and Class Members had no idea their PII had been stolen, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Defendant disregarded the rights of Plaintiff and the Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure their PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of

data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party.

11. Plaintiff brings this action on behalf of all persons whose PII was compromised because of Defendant's failure to: (i) adequately protect their PII; (ii) warn of Defendant's inadequate information security practices; and (iii) effectively secure equipment and the database containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and Class members have suffered actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach Incident; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach Incident; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' PII against theft and not allow access and misuse of their personal data by others; and (h) 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 Plaintiff's and Class Members' PII, and, at the very least, are entitled to nominal damages.

13. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

14. Plaintiff is, and at all times relevant hereto was, a citizen and resident of Cook County, Illinois.

15. Defendant is, and at all times relevant hereto was, a corporation with its principal place of business in Cook County, Illinois.

JURISDICTION AND VENUE

16. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant does business within this State and because Plaintiff's claims arise out of Defendant's actions which occurred in this State.

17. Venue is proper in this County pursuant to 735 ILCS 5/2-101, because Defendant conducts business in this County and thus resides there under § 2-102.

FACTS

18. At the time of the Data Breach Incident, Defendant maintained Plaintiff's and the Class members PII in its database and systems.

19. By obtaining, collecting, and storing Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

20. Plaintiff and Class members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

21. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class members' PII from involuntary disclosure to third parties.

22. Prior to the Data Breach Incident, Defendant should have (i) encrypted or tokenized the sensitive PII of Plaintiff and the Class members, (ii) deleted such PII that it no longer had reason to maintain, (iii) eliminated the potential accessibility of the PII from the internet and its website where such accessibility was not justified, and (iv) otherwise reviewed and improved the security of its network system that contained the PII.

23. Prior to the Data Breach Incident, on information and belief, Defendant did not (i) encrypt or tokenize the sensitive PII of Plaintiff and the Class members, (ii) delete such PII that it no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet and its website where such accessibility was not justified, and (iv) otherwise review and improve the security of its network system that contained the PII.

24. On or around May 29, 2023, an intruder gained unauthorized access to Defendant's database.

25. On or about April 17, 2024, – over a year after the actual event- Defendant mailed Plaintiff and the Class members a form notice attempting to minimize the Data Breach Event, while admitting that sensitive PII had been compromised and stolen.

26. Contrary to the self-serving narrative in Defendant's form notice, Plaintiff's and Class members' unencrypted information may end up for sale on the dark web and/or fall into the hands of companies that will use the detailed PII for targeted marketing without approval.

27. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and the Class members.

28. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII, relied on Defendant to keep their PII confidential and securely maintained,

to use this information for business purposes only, and to make only authorized disclosures of this information.

29. Defendant could have prevented the Data Breach Incident by properly securing and encrypting Plaintiff's and Class members' PII, or Defendant could have destroyed the data, especially old data from former inquiries and/or customers that Defendant had no legal right or responsibility to retain.

30. Defendant's negligence in safeguarding Plaintiff's and the Class members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in the financial sector.

31. Despite the prevalence of public announcements and knowledge of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the Class members from being compromised.

32. The ramifications of Defendant's failure to keep secure Plaintiff's and the Class members' PII 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.

33. Social Security numbers, for example, are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

34. Even more problematic, 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 evidence of actual, ongoing fraud activity to obtain a new number.

35. The PII of Plaintiff and the Class Members was stolen to engage in identity theft and/or to sell it to criminals who will purchase the PII for that purpose.

36. Moreover, 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.

37. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and the Class members' PII, 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 Plaintiff and the Class members as a result of a breach.

38. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

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

40. The injuries to Plaintiff and the Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Plaintiff's and the Class members' PII.

41. Plaintiff has suffered and will continue to suffer injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third-parties and criminals.

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

CLASS ALLEGATIONS

PROPOSED CLASS

43. Plaintiff brings this lawsuit as a class action on behalf individually and on behalf of all other similarly situated persons as a class action pursuant to 735 ILCS § 5/2-801. The "Class" that Plaintiff seeks to represent is defined as:

> **All persons whose PII was accessed and/or exfiltrated during the Data Breach Incident.**

NUMEROSITY

44. The Data Breach Incident has impacted at least 1,000 persons. The members of the Class, therefore, are so numerous that joinder of all members is impracticable.

45. Identification of the Class members is a matter capable of ministerial determination from Defendant's records.

COMMON QUESTIONS OF LAW AND FACT

46. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are: [1] Whether and to what extent Defendant had a duty to protect the PII Plaintiff and Class members; [2] Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members; [3] When Defendant actually learned of the Data Incident; [4] Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised; [4] 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 Incident; [5] Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach Incident to occur; [6] Whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; [7] Whether

Plaintiff and the Class members are entitled to restitution as a result of Defendant's wrongful conduct; and [8] Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach Incident.

47. The common questions in this case are capable of having common answers. Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY

48. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

PROTECTING THE INTERESTS OF THE CLASS MEMBERS

49. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY

50. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class are in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct are too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

51. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For example, one court might enjoin Defendant from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

52. Plaintiff re-alleges and incorporates the allegations contained in paragraphs 1-52 as if fully set forth herein.

53. Defendant was provided and entrusted with certain PII, including Plaintiff's and the Class members' name, social security number, and medical information.

54. Plaintiff and the Class members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

55. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class members could and would suffer if the PII were wrongfully disclosed.

56. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of Plaintiff's and the Class members' PII involved an unreasonable risk of harm to Plaintiff and the Class members, even if the harm occurred through the criminal acts of a third party.

57. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing

Defendant's security protocols to ensure that Plaintiff's and the Class members' information in Defendant's possession was adequately secured and protected.

58. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain.

59. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class members' PII.

60. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class members. That special relationship arose because Plaintiff and the Class members entrusted Defendant with their confidential PII, a necessary part of obtaining treatment or employment from Defendant.

61. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiff and the Class members.

62. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

63. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

64. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach Incident as set forth herein. Defendant's misconduct also

included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class members' PII, including basic encryption techniques freely available to Defendant.

65. Plaintiff and the Class members had no ability to protect their PII that was in, and remains in, Defendant's possession.

66. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class members as a result of the Data Breach Incident.

67. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

68. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class members.

69. Defendant has admitted that the PII of Plaintiff and the Class members was wrongfully accessed by and exfiltrated by unauthorized third persons.

70. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class members during the time the PII was within Defendant's possession or control.

71. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach Incident.

72. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect Plaintiff's and the Class members' PII in the face of increased risk of theft.

73. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class members by failing to have appropriate procedures in place to detect and prevent dissemination of their PII.

74. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Plaintiff's and the Class members' PII it was no longer required to retain.

75. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class members the existence and scope of the Data Breach Incident.

76. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class members, the PII of Plaintiff and the Class members would not have been compromised.

77. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class members and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class members. Plaintiff's and the Class members' PII was accessed and exfiltrated as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

78. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class members have suffered and will suffer injury, including but not limited to: (i) threat of identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach Incident, including but

not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on bank accounts and credit reports; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and the Class members' PII; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach Incident for the remainder of the lives of Plaintiff and the Class members.

79. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

80. Additionally, as a direct and proximate result of Defendant's negligence , Plaintiff and the Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

81. As a direct and proximate result of Defendant's negligence ,

Plaintiff and the Class members are at an increased risk of identity theft or fraud.

82. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class members are entitled to and demand actual consequential, and nominal damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

a) An order certifying this case as a class action on behalf of the Class as defined above, and appointing Plaintiff as the representative of the Class and Plaintiff's counsel as Class Counsel;

b) Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class members;

c) Injunctive relief, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order: (1) 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; (2) requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff 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 Plaintiff and Class Members; (3) requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Member's personal identifying information; (4) prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database; (5) 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; (6) requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring; (7) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (8) 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; (9) requiring Defendant to conduct regular database scanning and securing checks; (10) 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 personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members; (11) 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; (12) 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 personal identifying information; (13) 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; (14) requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; (15) requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and (16) for a period of 10 years, appointing a qualified and independent third party assessor to conduct 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;

d) For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f) For prejudgment interest on all amounts awarded; and

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

DATED: October 30, 2024

Respectfully submitted,

HAMMERVOLD LAW, LLC

/s/ Mark Hammervold
Mark Hammervold
IL Bar No. 6320744
155 S. Lawndale Ave.
Elmhurst, IL 60126
(405) 509-0372
mark@hammervoldlaw.com

DAPEER LAW, P.A.

/s/ Rachel Dapeer
Rachel Dapeer
ARDC No. 6337367
**Pro Hac Forthcoming*
20900 NE 30th Ave #417
Aventura, FL33180
954-799-5914
rachel@dapeer.com

Attorneys for Plaintiff and the Putative Class