**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF TEXAS**
**SHERMAN DIVISION**

| | |
|---|---|
| MICHELLE JINKS, individually, and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>MARQUIS SOFTWARE SOLUTIONS, INC.,<br><br>Defendant. | Case No. 4:25-cv-01277<br><br>**JURY TRIAL DEMANDED** |

**CLASS ACTION COMPLAINT**

Plaintiff Michelle Jinks, individually, and on behalf of all similarly situated persons, alleges the following against Marquis Software Solutions, Inc. ("Marquis" or "Defendant"), based on Plaintiff's own personal knowledge and on information and belief derived from, among other things, investigation by counsel and review of public documents, as to all other matters:

## I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' ("Class Members," as defined *infra*) sensitive personally identifiable information—i.e., information that is or could be used, whether on its own or in combination with other information, to identify, locate, or contact a person, including, without limitation: dates of birth, account numbers, Social Security Numbers, and Tax Identification Numbers.

2. Defendant Marquis is a marketing and compliance software and services provider

that specializes in providing services to banks and credit unions.[1]

3. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant by financial institutions on the mutual understanding that Defendant would protect it against disclosure—was targeted, compromised and unlawfully accessed due to the Data Breach.

4. The information compromised in the Data Breach included Plaintiff's and Class Members' dates of birth, account numbers, Social Security Numbers, and Tax Identification Numbers ("Private Information").

5. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) adequately vet its data security practices; (ii) warn Plaintiff and Class Members of Marquis's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in their hands.

7. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a technology vendor that collects and maintains highly valuable Private Information on its servers and systems.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect the Private

[1] *See* https://gomarquis.com/.

Information in its possession from a foreseeable and preventable cyber-attack.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to ensure that they had adequate and reasonable safeguards and measures in place to protect the Private Information of Plaintiff and Class Members after that information was transferred and entrusted to it in the regular course of business. More specifically, Defendant failed to take and implement available steps to prevent an unauthorized disclosure of data, and failed to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption, storage, and destruction of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to unknown and unauthorized third parties.

10. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe in any further transfers of their sensitive data to third parties and they should be entitled to injunctive and other equitable relief.

11. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained has been accessed and acquired by data thieves.

12. As a result of the Data Breach, Plaintiff on information and belief thousands of Class Members suffered concrete injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) Plaintiff's Private Information being at imminent risk of being disseminated on the Dark Web; (vii) experiencing an increase in spam calls, texts,

and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

13. Armed with the Private Information accessed in the Data Breach, data thieves can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

16. Through this Complaint, Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

## II. PARTIES

***Plaintiff Michelle Jinks***

17. Plaintiff is an adult citizen of the state of Louisiana, where she intends to remain.

18. Plaintiff's provided Private Information was provide to Marquis as a condition of receiving services.

19. Plaintiff trusted that Defendant and its customers would use reasonable measures to protect her Private Information—according to its policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

20. At the time of the Data Breach, Defendant collected and retained Plaintiff's and Class Members' Private Information in its servers and systems.

21. Plaintiff's and Class Members' Private Information was compromised in the Data Breach and stolen by cybercriminals in a targeted attack.

22. Plaintiff has been injured by the compromise of her Private Information.

23. Plaintiff takes reasonable measures to protect her Private Information.

24. Plaintiff stores any documents containing Private Information in a safe and secure location and diligently chooses unique usernames and passwords for online accounts.

25. Had Plaintiff known that Defendant does not adequately protect Private Information, Plaintiff would not have agreed to provide sensitive Private Information to Defendant and would not have agreed to the use of Defendant's services.

26. As a result of and following the Data Breach, Plaintiff has suffered a loss of time and has spent, and continues to spend, a considerable amount of time on issues related to this Data

Breach to protect herself from identity theft and fraud. Plaintiff has monitored, and continues to monitor, accounts, credit reports and credit scores, and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties. This time would not have been spent but for the Defendant's negligence.

27. In the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff fears for Plaintiff's personal financial security and worries about what information was exposed in the Data Breach. Because of the Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

28. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that was entrusted to Defendant, which was compromised in and as a result of the Data Breach.

29. Plaintiff suffered uncompensated lost time and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy.

30. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Plaintiff's Private Information being placed in the hands of criminals that will continue for Plaintiff's lifetime.

31. Defendant obtained and continues to maintain Plaintiff's Private Information and thus has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

32. As a result of the Data Breach, Plaintiff anticipates spending considerable time and

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

33. Further, Plaintiff is and will remain at risk of harm in the future because Defendant continues to maintain Plaintiff's confidential Private Information but has not taken adequate steps to protect that information from a future data breach. Accordingly, Plaintiff's Private Information continues to face an imminent risk of unauthorized disclosure from a future data breach of Marquis.

***Defendant Marquis Software Solutions, Inc.***

34. Defendant Marquis, based in Plano, Texas, provides software and services to over 500 banks and credit unions[2], including marketing, compliance, analytics, CRM, digital communications, and integrations.

35. Defendant is a corporation with its principal place of business located at 6509 Windcrest Drive, Suite 170, Plano, Texas 75024 in the Sherman Division of the Eastern District of Texas. The registered agent for service of process is C.T. Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. Defendant is a citizen of Texas.

## III. JURISDICTION AND VENUE

36. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) the Plaintiff and numerous Class Members are diverse from Defendant, and (4) there are more than 100 Class Members. Defendant is a citizen of Texas.

37. The Court has general personal jurisdiction over Defendant because Defendant has

[2] *See* https://gomarquis.com/.

its principal place of business in the Sherman Division of the Eastern District of Texas.

38. Venue is proper in this District of Texas pursuant to 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in the Sherman Division of the Eastern District of Texas, and much of the conduct alleged in this complaint is believed to have occurred in this Division and District.

## IV. FACTUAL ALLEGATIONS

### A. *Defendant's Business*

39. Marquis is a technology vendor serving hundreds of banks and credit unions.

40. Plaintiff and Class Members are current and former customers of the financial institutions that utilize Marquis's services.

41. In the regular course of its business, Marquis receives and handles Private Information, which includes, *inter alia*, consumers' full name, address, date of birth, tax identification numbers, Social Security number, financial account and payment card information, and other sensitive information from their customers and other individuals who interact or otherwise transact with Marquis for business purposes.

42. Defendant stores this highly sensitive information digitally.

43. Plaintiff and Plaintiff's financial institution entrusted this 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.

44. By obtaining, collecting, and storing Plaintiff's Private Information, Defendant assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiff's Private Information from unauthorized disclosure.

45. Plaintiff and Class Members have taken reasonable steps to maintain the

confidentiality of their Private Information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

46. Defendant has a statutory and common law duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its customers' Private Information safe and confidential.

47. Defendant has obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

48. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

**B. *The Data Breach***

50. Marquis detected the suspicious activity on its computer network in August 2025, indicating a data breach.

51. The company claims to have launched an investigation and engage cybersecurity experts to assess the situation. The company also notified law enforcement and began working with affected financial institutions to identify impacted individuals. Based on a subsequent forensic investigation, Marquis determined that an unauthorized third party accessed its network and may

have accessed and acquired certain files from its systems.

52. On or about November 17, 2025, Marquis began sending victims a Notice of Data Breach letter (the "Notice Letter")[3], informing them that:

> **What Happened**
>
> On August 14, 2025, we identified suspicious activity on our network and later determined that it was the result of a cybersecurity incident. Upon learning of the incident, we immediately launched an investigation and engaged the appropriate cybersecurity experts to assist. We also promptly notified law enforcement. Our investigation determined that an unauthorized third party accessed our network and may have accessed and acquired certain files from our systems. Importantly, [Data Owner or Entity]'s internal systems were not impacted; the incident was limited to the vendor's environment.
>
> **What Information Was Involved**
>
> We reviewed the contents of the copied files to determine if they contained any personal information. On October 27, 2025, we determined that the following data of yours was included in the copied files: [Breached Elements]. At this time, we have no evidence of the misuse, or attempted misuse, of personal information as a result of this incident.

53. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

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

55. According to Marquis, the Private Information accessed by cybercriminals

[3] A copy of the template Notice Letter is attached hereto as Exhibit A.

involved a wide variety of Private Information, including dates of birth, account numbers, Social Security Numbers, and Tax Identification Numbers.[4]

56. Despite the breadth and sensitivity of the Private Information that was exposed, and the attendant consequences to customers as a result of the exposure, Marquis failed to disclose the Data Breach for months from the time of the Breach. This inexplicable delay and further exacerbated the harms to Plaintiff and Class Members.

57. Based on the Notice Letter, the type of cyberattack involved, and public news reports, and reliable information received by the Plaintiff, her Private Information was stolen in the Data Breach.

58. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Private Information and has engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiff's and Class Member's Private Information on the dark web.

59. Accordingly, Defendant had obligations created by industry standards, common law and statutory law to keep Plaintiff and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

60. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive personal information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information. Nor did Defendant take the precautions and measures needed to ensure Marquis's data security protocols were sufficient to protect the Private Information in its possession.

61. The attacker accessed and acquired files containing unencrypted Private

[4] *Id.*

Information of Plaintiff and Class Members. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

62. Plaintiff further believes Plaintiff's Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

### C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information*

63. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[5]

64. Defendant derives a substantial economic benefit from providing services to its customers, and as a part of providing those services, Defendant retains and stores the Private Information of its customers and of other individuals who directly or indirectly interact or otherwise transact with Marquis for business purposes, including that of Plaintiff and Class Members.

65. By obtaining, collecting, and storing the PII/PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the Private Information from disclosure.

66. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

67. Defendant could have prevented this Data Breach by properly securing the Private

[5] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on Nov. 19, 2025).

Information of Plaintiff and Class Members.

68. Upon information and belief, Defendant made promises to its customers and consumers to maintain and protect Private Information, demonstrating an understanding of the importance of securing Private Information.

69. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

**D. *Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of Private Information Are Particularly Susceptible to Cyberattacks***

70. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

71. As here Data thieves regularly target companies that receive and maintain Private Information due to the highly sensitive nature of that information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access in targeted attacks.

72. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

73. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it collected and maintained and, thus, the significant number of individuals who would be harmed by the exposure of that data.

74. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

75. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

76. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

**E.** ***Value of Personally Identifiable Information***

77. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[7]

78. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[8]

---

[6] 17 C.F.R. § 248.201 (2016).
[7] *Id.*
[8] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

79. Criminals can purchase access to entire company data breaches from $900 to $4,500.[9]

80. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change. Particularly so with a person's social security number, the prime ingredient for identity theft.

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

82. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used.

**F. *Defendant Failed to Comply with FTC Guidelines***

83. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

84. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on

[9] *In the Dark*, VPNOVERVIEW.COM, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 19, 2025).

computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

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

87. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

88. Defendant was at all times fully aware of its obligation to protect the Private Information it was entrusted with yet failed to comply with such obligation. Defendant was also aware of the significant repercussions that would result from their failure to do so.

### G. *Defendant Failed to Comply with Industry Standards*

89. As noted above, experts studying cybersecurity routinely identify institutions like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which it collects and maintains.

90. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Marquis, include, but are not limited to: educating all employees; strong password requirements; multilayer security, including firewalls; anti-virus and anti-malware software; encryption; multi-factor authentication; backing up data; and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all these industry best practices.

91. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

92. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

### H. *Defendant Breached Its Duty to Safeguard Plaintiff's and Class Members' Private Information*

93. In addition to their obligations under federal laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty

to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

94. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

95. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

96. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

97. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. 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 that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' and other related individuals' Private Information;

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

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class

Members' Private Information.

98. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

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

**I.** ***Common Injuries & Damages***

100. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of the value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, 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' Private Information.

**J.** ***The Data Breach Increases Victims' Risk of Identity Theft***

101. Plaintiff and Class Members are at an imminent and heightened risk of identity theft for years to come.

102. The unencrypted Private Information of Class Members has or will end up for sale

on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

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

104. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

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

106. One such example of criminals piecing together bits and pieces of compromised

Private Information for profit is the development of "Fullz" packages.[10]

107. With "Fullz" packages, cybercriminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

108. The development of "Fullz" packages means that the stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, driver's license numbers, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

**K.** ***Loss of Time to Mitigate Risk of Identity Theft and Fraud***

109. As a result of the recognized risk of identity theft, when a data breach occurs, an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the

[10] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KREBSONSECURITY.COM BLOG (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

110. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect.

111. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

112. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

### L. *Diminution of Value of Private Information*

113. Private Information is a valuable property right. Its value is axiomatic, considering

---

[11] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf

[12] *See* Federal Trade Commission, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited Nov. 19, 2025).

the value of Big Data in corporate America and the consequences of cyberthefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

114. An active and robust legitimate marketplace for Private Information exists.

115. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[13]

116. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

### M. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary*

117. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will imminently be placed, on the black market/Dark Web for sale and purchased by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

[13] DATACOUP, https://datacoup.com/ (last visited Nov. 19, 2025).

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

119. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

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

**N. *Plaintiff's Experience***

121. Plaintiff provided her Private Information to CSE Federal Credit Union, one of Marquis's financial institution customers, along with (it is believed) some 32,000 others.

122. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. There is no reason to believe it is.

123. At the time of the Data Breach, Defendant collected and retained Plaintiff's and Class Members' Private Information in its systems.

124. Plaintiff's and Class Members' Private Information was compromised in the Data Breach and stolen by cybercriminals.

125. Plaintiff has been injured by the compromise of Plaintiff's Private Information.

126. Plaintiff takes reasonable measures to protect her Private Information.

127. Plaintiff stores any documents containing Private Information in a safe and secure location and diligently chooses unique usernames and passwords for online accounts.

128. Had Plaintiff known that Defendant does not adequately protect Private Information, Plaintiff would not have allowed her sensitive Private Information to be provided to Defendant.

129. As a result of and following the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach to protect Plaintiff from identity theft and fraud. Plaintiff has monitored, and continues to monitor, accounts, credit reports and credit scores, and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties. This uncompensated time spent by the Plaintiff would not have occurred but for the Defendant's negligence.

130. In the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam text messages and phone calls. Plaintiff fears for Plaintiff's personal financial security and worries about what information was exposed in the Data Breach. Because of the Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

131. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information —a form of intangible property that was entrusted to Defendant, which was compromised in and as a result of the Data Breach.

132. Plaintiff suffered uncompensated lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy.

133. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Plaintiff's Private Information being placed in the hands of criminals that will continue for Plaintiff lifetime.

134. Defendant obtained and continues to maintain Plaintiff's Private Information and thus has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

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

136. Further, Plaintiff is and will remain at risk of harm in the future because Defendant continues to maintain and store Plaintiff's confidential Private Information but has not taken adequate steps to protect that sensitive information from a data breach. Accordingly, Plaintiff's Private Information faces an imminent risk of disclosure in a future Marquis data breach.

## V. CLASS ALLEGATIONS

137. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks certification of the following class:

**Nationwide Class**

All individuals residing in the United States whose Private Information was compromised in the Marquis Software Solutions Data Breach, including all individuals who received notice of the Data Breach.

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

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

140. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

141. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but can and will be ascertained from Defendant's records.

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

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

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

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

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

g. Whether Defendant breached its duties to Class Members to safeguard their Private Information;

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

i. Whether Defendant had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant knew or should have known their data security systems and monitoring processes were deficient;

l. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

m. Whether Defendant's conduct was negligent;

n. Whether Defendant breached implied contracts with Plaintiff and Class Members or under a theory of them being a third party beneficiary of a contract;

o. Whether Defendant was unjustly enriched;

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

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

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

143. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Defendant's common misconduct. Plaintiff is advancing the same claims and legal theories on behalf of Plaintiff and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

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

146. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high

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

147. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

148. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names, email and/or postal addresses, and phone numbers of Class Members affected by the Data Breach.

## CLAIMS FOR RELIEF

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

149. Plaintiff realleges and incorporates by reference paragraphs 1-148 as if fully set forth herein.

150. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

151. Moreover, Defendant has a duty to promptly and adequately notify Plaintiff and

Class Members of the Data Breach.

152. Defendant has and continues to have duties to adequately disclose that the Private Information of Plaintiff and Class Members within Defendant's custody, control or 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 Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties. To date it has not in violation of the law.

153. Defendant breached its duties and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

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

b. Allowing unauthorized access to Class Members' Private Information;

c. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

d. Failing to remove former customers' Private Information it was no longer required to retain pursuant to regulations; and

e. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages. This still has not been done in accordance with the law at this time.

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

155. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches at large corporations that collect and store Private Information.

156. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

157. Plaintiff and 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 Private Information of Plaintiff and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on its servers and/or systems.

158. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

159. Plaintiff and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession, custody, or control.

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

161. Defendant's duties extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of

a specific duty to reasonably safeguard personal information.

162. Defendant has admitted that the Private Information of Plaintiff and Class Members were wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

163. But for Defendant's wrongful and negligent breaches the Private Information of Plaintiff and Class Members would not have been compromised.

164. There is a close causal connection between Defendant's failure to implement security measures to adequately protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in securing and safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

165. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's care, custody, control or possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

167. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's care, custody, control or possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

168. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

169. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

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

**COUNT II**
**Negligence *Per Se***
**(On Behalf of Plaintiff and the Nationwide Class)**

171. Plaintiff realleges and incorporates by reference paragraphs 1-170 as if fully set forth herein.

172. Defendant's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure Private Information.

173. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

174. Defendant's violations of Section 5 of the FTCA constitutes negligence *per se*.

175. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

176. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

177. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

178. The injury and harm that Plaintiff and the other Class Members' suffered was the direct and proximate result of Defendant's violations of law, including Section 5 of the FTCA. Plaintiff and Class Members' have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii)

breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) uncompensated lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

**COUNT III**
**Breach of Third-Party Beneficiary Contract**
**(On Behalf of Plaintiff and the Nationwide Class)**

179. Plaintiff re-alleges and incorporates by reference paragraphs 1–178 above as if fully set forth herein.

180. Defendant entered into uniform written contracts with its customers, including Plaintiffs' and Class Members' financial institutions, to provide third-party administrative services for Defendant.

181. Pursuant these contracts, Defendant received from its customers and maintained Plaintiffs' and Class Members' Private Information in the course of performing its contractual services, which it could not perform without receiving and maintaining such Private Information.

182. Pursuant to these contracts, Defendant's customers agreed to provide Defendant with compensation and Plaintiffs' and Class Members' Private Information.

183. In exchange, Defendant agreed, in part, to implement adequate data security measures to safeguard Plaintiffs' and Class Members' Private Information from unauthorized disclosure, and to timely notify Plaintiffs and Class Members of the Data Breach.

184. Defendant was required by statutes and regulations, including but not limited to the FTC Act, and state consumer privacy and protection laws, to have contracts with its clients that required Defendant to implement and maintain reasonable security procedures and practices to

protect its clients' customers'—Plaintiffs and Class Members—Private Information from unauthorized access, use, or disclosure.

185. The relevant statutes and regulations obligating Defendant to promise by contract to use reasonable data security for Plaintiff's and Class Members' Private Information create a class of intended beneficiaries whose members are implied into such agreements by operation of law. Plaintiff and Class Members are the intended beneficiaries of the contracts that Defendant entered into with Plaintiff's and Class Members' benefit plans to satisfy these statutory and regulatory requirements.

186. Upon information and belief, Defendant's contracts with its customers each contained a provision requiring Defendant to implement and maintain reasonable security procedures and practices appropriate to the nature of Private Information Defendant collected, to protect the Private Information from unauthorized access, use, or disclosure.

187. These contracts between Defendant and its customers were made expressly for the benefit of Plaintiff and Class Members as the intended third-party beneficiaries of these contracts.

188. Defendant knew Plaintiff and Class Members were involved and would benefit from the transactions that were subject to these contracts between Defendant's clients and Defendant.

189. Defendant knew that if it breached its contractual obligation to adequately safeguard Plaintiff's and Class Members' Private Information, Plaintiff and Class Members would be harmed.

190. Defendant breached these contracts with Plaintiff and Class Members' financial institutions, by, among other acts and omissions: (a) failing to use reasonable data security measures, (b) failing to implement adequate protocols and employee training sufficient to protect

Plaintiff's and Class Members' Private Information from unauthorized disclosure, and (c) failing to promptly or adequately notify Plaintiff and Class Members of the Data Breach.

191. As a direct and proximate result of Defendant's breaches of these contracts with its clients, Plaintiff and Class Members have suffered and will continue to suffer injuries as set forth herein and are entitled to damages sufficient to compensate for the losses they sustained.

**COUNT IV**
**Unjust Enrichment**
**(On Behalf of Plaintiff and the Nationwide Class)**

192. Plaintiff realleges and incorporates by reference paragraphs 1-191 as if fully set forth herein.

193. This count is brought in the alternative to Plaintiff's breach of contract claims.

194. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made by or on behalf of its customers, like Plaintiff's financial institution, for services.

195. As such, a portion of the value and monies derived from payments made by its customers for services is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

196. Plaintiff and Class Members conferred a monetary benefit on Defendant in providing it with their valuable Private Information.

197. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

198. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private

Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profit over the requisite security.

199. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

200. Under the principles of equity and good conscience, Defendant should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon it.

201. Plaintiff and Class Members have no adequate remedy at law.

202. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's custody, control or possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

203. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other

compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of Plaintiff and Class Members, requests judgment against Defendant and that the Court enter an Order:

A. Certifying this action as a class action and appointing Plaintiff and counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. Granting equitable relief and enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. Granting injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

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

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

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

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

H. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all issues so triable.

Dated: November 21, 2025

Respectfully submitted,

*/s/ Joe Kendall*
JOE KENDALL
Texas Bar No. 11260700
**KENDALL LAW GROUP, PLLC**
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Tel: 214-744-3000
Fax: 214-744-3015
E: jkendall@kendalllawgroup.com

Jonathan S. Mann (*pro hac vice* forthcoming)
**PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.**
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Fax: (205) 328-2711
E: jonm@pittmandutton.com

*Counsel for Plaintiff and the Putative Class*