UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

DANIEL HART, on behalf of himself and all others similarly situated, Plaintiff, v. MARQUIS SOFTWARE SOLUTIONS, INC. and NORWAY SAVINGS BANK, Defendants.	Case No. _____ **CLASS ACTION** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Daniel Hart ("Plaintiff"), on behalf of himself and all others similarly situated, brings this Class Action Complaint (the "Action") against the above-captioned Defendants, Marquis Software Solutions, Inc. ("Marquis") and Norway Savings Bank ("Norway" and, together with Marquis, "Defendants"), and alleges upon personal knowledge as to himself and his own actions, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard personally identifiable information entrusted to them by Class Members.

2. Multiple consumer-facing banks and credit unions, including Norway, recently reported a data breach of Marquis that occurred in August 2025. The data breach compromised personally identifiable information of tens or hundreds of thousands of individuals (if not many more), including roughly 51,000 current and former customers of Norway, nearly 7,000 customers

of Community 1st Credit Union, and numerous customers of CSE Federal Credit Union.

3. The information compromised in the Data Breach (as defined below) is extensive and includes at least names and addresses; dates of birth; account numbers; Social Security Numbers; tax ID numbers; and financial account information (collectively, "PII").

4. Defendants, as substantial businesses, had the resources to take seriously the obligation to protect private information. However, Defendants failed to invest the resources necessary to protect the PII of Plaintiff and Class members.

5. The actions of Defendants related to this Data Breach (as defined below) are unconscionable. Upon information and belief, Marquis failed to implement practices and systems in order to mitigate against the risks posed by Marquis's negligent (if not reckless) IT practices. Norway, in turn, negligently entrusted Marquis with Plaintiff's and the Class members' PII. As a result of these failures, Plaintiff and Class members face a litany of harms that accompany data breaches of this magnitude and severity.

6. As such, Plaintiff, on behalf of himself and all others similarly situated, brings this Action for restitution, actual damages, nominal damages, statutory damages, injunctive relief, disgorgement of profits, and all other relief that this Court deems just and proper.

II. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs; there are more than 100 putative Class members; and minimal diversity exists because one or more putative Class members are citizens of a different state than Defendants.

8. This Court has personal jurisdiction over Marquis because Marquis maintains its

principal place of business and operations in Texas, because Marquis intentionally availed itself of this jurisdiction by regularly conducting business and providing employment in Texas, and because Marquis's acts and omissions giving rise to Plaintiff's and the Class's claims occurred in and emanated from Texas.

9. This Court has personal jurisdiction over Norway because it has intentionally availed itself of this jurisdiction by employing Marquis services, and because Norway's acts and omissions in employing Marquis's services give rise to Plaintiff's and the Class's claims, thus emanating from Texas.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Marquis's principal place of business is at 6509 Windcrest Dr, Suite 170, Plano, TX 75024; because Marquis operates extensively in this District; and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

III. PARTIES

Plaintiff

11. Plaintiff is a citizen of the state of Maine. Plaintiff is a customer of Norway Savings Bank whose information was compromised in the Data Breach.

Defendant Marquis

12. Defendant Marquis is a technology vendor serving hundreds of banks and credit unions across the United States. Marquis's headquarters are located at 6509 Windcrest Drive, Suite 180, Plano, Texas 75024.

Defendant Norway Savings Bank

13. Defendant Norway Savings Bank provides mutual banking and financial services in Maine. Norway Savings Bank's headquarters are located at 261 Main Street, Norway, Maine 04268.

IV. FACTUAL ALLEGATIONS

A. Defendants' Business and Collection of Private Information

14. Norway and numerous other banks and credit unions utilized Marquis's technology vendor services for a variety of purposes, including the storage of Plaintiff's and Class members' PII. Plaintiff's and the Class members' PII was given to and entrusted to Norway and numerous other banks and credit unions for banking purposes. In undertaking this responsibility, Norway and the other banks and credit unions who engaged Marquis were obligated to hire only vendors who maintain adequate data security practices.

15. In the ordinary course of receiving banking services from Norway and other clients of Marquis, customers are required to provide, at a minimum, their PII.

16. In the course of doing business, Marquis acquires a significant amount of highly sensitive and valuable private information from the customers of financial institutions (such as Norway) that utilize Marquis's services, including the acquisition of the PII of Plaintiff and Class members.

17. As a condition of receiving this PII, Plaintiff and Class members trusted that Norway and the other banks and credit unions that engaged Marquis would use their data only for business purposes in a manner that was safe and secure and would entrust their PII only to third-party vendors that are safe and secure.

18. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class

members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for ensuring the safety and security of Plaintiff's and Class members' PII and for protecting such PII from unauthorized disclosure and exfiltration.

19. Plaintiff and Class members relied on Defendants 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.

B. The Data Breach

20. As noted, in August 2025, Marquis experienced a cyberattack in which the PII of tens or hundreds of thousands (if not many more) of current or former customers of banks and credit unions that engaged Marquis—including roughly 51,000 customers of Norway Savings Bank, nearly 7,000 customers of Community 1st Credit Union, and various customers of CSE Federal Credit Union, among others—was compromised and exfiltrated (the "Data Breach").

21. Not only do Plaintiff and Class members have to contend with the harms caused by the Data Breach, but Defendants' response to the Data Breach has been woefully insufficient. In fact, Marquis has yet to issue a notice to all impacted customers. And even though the Data Breach occurred on August 25, 2025, Norway did not begin notifying applicable authorities or impacted victims until the past few days.

22. On information and belief, the PII compromised in the files accessed by the cybercriminals who perpetrated the Data Breach was not encrypted. In any event, the cybercriminals were able to access the PII enumerated above.

23. The removal of PII from Marquis's systems demonstrates that this cyberattack was orchestrated due to Marquis's status as a business that houses sensitive PII. Armed with this PII, data thieves (as well as downstream purchasers of the stolen PII), can commit a variety of crimes,

including: 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' identification information, obtaining driver's licenses in Class members' names but with different photographs, and giving false information to police during any arrests.

24. Due to Marquis's flawed security measures and Defendants' incompetent response to the Data Breach, Plaintiff and Class members now face a present, substantial, and imminent risk of fraud and identity theft and must deal with that threat forever.

25. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, and despite Defendants large operating budgets, Defendants provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling PII, as well as inadequate employee training regarding how to access, how to oversee the protection of, and how to handle and safeguard this sensitive set of information.

26. Defendants failed to adequately adopt and train their employees on even the most basic of information security protocols, including storing, locking, encrypting, and limiting access to the highly sensitive PII of customers; implementing guidelines for accessing, maintaining, and communicating sensitive PII; and protecting sensitive PII by implementing protocols on how to utilize such information.

27. Defendants' collective failures caused the unpermitted disclosure of Plaintiff's and Class members' PII to unauthorized third-party cybercriminals and put Plaintiff and Class members at serious, immediate, and continuous risk of identity theft and fraud.

28. The Data Breach that exposed Plaintiff's and Class members' PII was caused by

Defendants' violation of their obligations to abide by best practices and industry standards concerning their information security practices and processes.

29. Defendants, despite being technologically advanced organizations, failed to comply with basic security standards or to implement security measures that could have prevented or mitigated the Data Breach.

30. Defendants failed to ensure that all personnel with access to PII were properly trained in retrieving, handling, using, and distributing sensitive information. Marquis's personnel were also not properly trained to apply relevant updates and software patches.

C. The Data Breach Was Foreseeable

31. Defendants both had weighty obligations created by industry standards, common law, and their own promises and representations to keep PII confidential and to protect it from unauthorized access and disclosure.

32. Plaintiff and Class members provided their PII to Norway—and to other banks and credit unions who engaged Marquis as a vendor—with the reasonable expectation and mutual understanding that their third-party vendors, including Marquis, would comply with their obligations to keep such information confidential and secure from unauthorized access.

33. Defendants' data security obligations were particularly acute given the substantial increase in ransomware attacks and/or other data breaches in various industries—including financial industries—preceding the date of the Data Breach.

34. Defendants were aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

35. PII, like the PII targeted by the hackers in this Action, is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of

unlawful manners. For example, PII can be used to distinguish, identify, or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

36. Given the nature of the Data Breach, it is foreseeable that the compromised PII can now be used by hackers and cybercriminals in a variety of different and harmful ways.

37. Cybercriminals who possess Class members' PII can (in isolation or in tandem with other information) obtain Class members' tax returns or open fraudulent credit card or other types of accounts in Class members' names.

38. The increase in such attacks, and attendant risk of future attacks, was widely known to Defendants.

39. As such, this Data Breach was foreseeable. Defendants were cognizant of the significant risk of data breaches because of how common and high-profile data breaches have become with respect to businesses, such as Defendants.

D. Defendants Failed to Follow FTC Guidelines and Industry Standards

40. Experts studying cybersecurity routinely identify consumer-facing businesses, such as Defendants, as being particularly vulnerable to cyberattacks because of the value of the data which they collect and maintain. The reason this data is so valuable is because it contains PII, which can be sold and weaponized for purposes of committing various identity theft-related crimes. It is well-known that, because of the value of this data and PII, businesses that collect, store, maintain, and otherwise utilize or profit from PII must take necessary cybersecurity safeguards to ensure that the data they possess is adequately protected.

41. Government agencies also highlight the importance of cybersecurity practices. For

example, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

42. According to the FTC, the need for data security should be factored into all business decision-making.

43. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

44. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand network vulnerabilities; and implement policies to correct any security problems.

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

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

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect sensitive personal data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15

U.S.C. § 45 ("FTCA"). Orders resulting from these actions further explicate and clarify the measures businesses must take to meet their data security obligations.

48. Defendants failed to properly implement some or all of these (and other) basic data security practices.

49. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

50. Defendants at all times were fully aware of their obligations to protect PII. Defendants were also keenly aware of the significant repercussions that would result from the failure to do so.

51. Several best practices have been identified that, at a minimum, should be implemented by businesses such as Defendants, include but are not limited to the following: educating all employees about cybersecurity; requiring strong passwords; maintaining multi-layer security, including firewalls, anti-virus programs, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

52. Other best cybersecurity practices that are standard in the industry 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 protection of physical security systems; and training staff regarding critical points.

53. These foregoing frameworks are existing and applicable industry standards. Defendants failed to comply with these accepted standards, thereby opening the door to and

causing the Data Breach.

E. Defendants' Breaches of Their Obligations

54. Defendants breached their obligations to Plaintiff and Class members and were otherwise negligent and/or reckless because Defendants failed to properly maintain, oversee, and safeguard their computer systems (and third-party vendor's computer systems), network, and data. In addition to their obligations under federal and state law, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class members to provide reasonable security, including complying with industry standards and requirements, providing training for their staff, and ensuring that their computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class members.

55. Defendants' wrongful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect the PII of current and former customers;

c. Failing to implement updates and patches in a timely manner;

d. Failing to properly monitor third-party data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

e. Failing to ensure that all employees and third-parties apply all available and necessary security updates;

f. Failing to ensure that all employees and third-parties install the latest software

patches, update their firewalls, check user account privileges, and ensure proper security practices;

g. Failing to ensure that all employees and third-parties practice the principle of least-privilege and maintain proper credential hygiene;

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to adequately oversee employees and third-party vendors;

j. Failing to ensure that all employees and third-parties employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

k. Failing to properly train and supervise employees and third-parties in the proper handling of inbound emails.

56. As the result of allowing their computer systems to fall into dire need of security upgrading and their inadequate procedures for handling cybersecurity threats, Defendants negligently and wrongfully failed to safeguard Plaintiff's and Class members' PII.

57. Accordingly, as further detailed herein, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their sensitive and personal information.

F. Data Breaches Are Harmful and Disruptive

58. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

59. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it because there is (unfortunately) a market for personally identifiable information, like the PII compromised

by the Data Breach.

60. Cybercriminals do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the greater number of accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim's identity, or otherwise to harass or track the victim.

61. 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 regarding a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls, deceptive text messages, and phishing emails.

62. Because of the threat of these harms, the FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and potentially obtaining an extended fraud alert that lasts for 7 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.

63. Theft of PII is gravely serious. PII is an extremely valuable property right.

64. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates that PII has considerable market value.

65. According to the GAO:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

66. Private information, such as the PII compromised herein, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. The private information of individuals remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, certain sets of private information can be sold at a price from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit card or debit card number can sell for between $5 and $110 on the dark web. Clearly, all this data has real value—which is why it is often targeted and stolen in the first place.

67. Because the PII compromised in the Data Breach has been dumped onto the dark web, Plaintiff and Class members are at a substantial imminent risk of injury, including an increased risk of fraud and identity theft for many years into the future.

68. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts and other indices of identity theft (*i.e.*, the mail, email, etc.) for many years to come.

G. Harm to Plaintiff and the Class

69. Plaintiff and Class members suffered actual injury from having their PII compromised as a result of the Data Breach, including, but not limited to, as follows: (a) misuse of their compromised PII; (b) damage to and diminution in the value of their PII, a form of property

that Defendants obtained from Plaintiff; (c) violation of their privacy, including the compromise of highly sensitive PII; (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential out-of-pocket losses including the loss of time.

V. CLASS ALLEGATIONS

70. Plaintiff brings this nationwide class on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure. The "Class" that Plaintiff seek to represent is defined as follows:

> **Class Definition.** All persons whose PII was maintained by Marquis and was compromised in the Data Breach.

71. Plaintiff also seeks to represent a subclass consisting of all individuals whose PII was entrusted to Norway, was maintained by Marquis, and was compromised in the Data Breach (the "Norway Subclass," and, together with the Class, the "Classes").

72. Excluded from the Classes are Defendants and Defendants' subsidiaries, affiliates, officers, and directors, and any entity in which Defendants have a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

73. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

74. **Numerosity**. The Data Breach compromised PII of tens or hundreds of thousands of individuals, if not many more, including roughly 51,000 current or former customers of Norway. Therefore, the members of the Classes are so numerous that joinder of all members is impractical.

75. **Commonality**. There are questions of law and fact common to the Class and/or the Norway Subclass, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

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

e. Whether Defendants owed a duty to Plaintiff and Class members to safeguard their PII;

f. Whether Defendants breached their duties to Plaintiff and Class members to safeguard their PII;

g. Whether computer hackers / cybercriminals obtained Plaintiff's and Class members' PII in the Data Breach;

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

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' acts, inactions, and practices complained of herein amount to a breach of contract, and/or common law negligence, and whether Defendants have been unjustly enriched;

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

l. Whether Plaintiff and Class members are entitled to damages, civil penalties, equitable relief, and/or injunctive relief.

76. **Typicality**. Plaintiff's claims are typical of those of other Class and Norway Subclass members because Plaintiff's PII, like that of every other Class and Norway Subclass member, was compromised in the Data Breach. Further, Plaintiff, like all Class members, was injured by the uniform conduct of Marquis, and, like all members of the Norway Subclass, was

injured by the uniform conduct of Norway. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class and Norway Subclass members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class and Norway Subclass members arise from the same operative facts and are based on the same legal theories.

77. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class and of the Norway Subclass in that he has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class or the Norway Subclass. The damages and infringement of rights that Plaintiff suffered are typical of the other Class and Norway Subclass members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class or the Norway Subclass. Plaintiff has retained counsel experienced in complex class action litigation, including data privacy class action litigation, and Plaintiff intends to prosecute this action vigorously.

78. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class or Norway Subclass members, and certification as a class action will preserve judicial resources by allowing the Classes' common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Classes will remain unaware of the claims they may possess.

79. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class and Norway Subclass members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

80. Adequate notice can be given to Class and Norway Subclass members directly using information maintained in Defendants' records.

81. **Predominance**. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendants have engaged in a common course of conduct toward Plaintiff and Class members and toward Plaintiff and Norway Subclass members. The common issues arising from Defendants' conduct affecting Class members and Norway Subclass members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

82. This proposed class action does not present any unique management difficulties.

COUNT I (Against All Defendants)

NEGLIGENCE

83. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

84. Norway knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the PII from being disclosed, compromised, lost, stolen, or misused by unauthorized parties.

85. This duty included obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Defendants' duties included the responsibility to design, implement, and monitor its data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

86. Norway and Marquis 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 their systems and networks, their policies, and procedures, and the personnel responsible for them adequately protected the PII.

87. Norway and Marquis owed a duty of care to safeguard the PII in light of the foreseeable risk of a data breach and the severe consequences that would result from their failure to so safeguard PII.

88. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and those individuals who entrusted them with their PII, which duty is recognized by laws and regulations, including but not limited the FTCA as well as common law. Defendants were in a position to ensure that their own systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class members from a Data Breach.

89. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the FTCA, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

90. Defendants' duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect PII that they acquire, maintain, or store.

91. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class members' PII, as alleged above.

92. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiff and Class members. Further, the breach of

security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in industries such as Defendants.

93. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

94. The imposition of a duty of care on Defendants to safeguard the PII they maintained, transferred, stored, or otherwise used is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiff and Class members as a result of the Data Breach.

95. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members are at a current and ongoing imminent risk of identity theft, and Plaintiff and Class members sustained compensatory damages including the following: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the material risk and imminent threat of identity theft; (iv) financial "out of pocket" costs incurred due to identity theft; (v) loss of time incurred due to identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their PII; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance, and nuisance, and (x) the continued risk to PII, which remains in Defendants' and the threat actors' respective control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

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

97. Defendants negligent conduct is ongoing, in that they still hold the PII of Plaintiff

and Class Members in an unsafe and unsecure manner.

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

COUNT II (Against Norway on Behalf of the Norway Subclass)

BREACH OF IMPLIED CONTRACT

99. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

100. Norway entered into contracts with customers to provide banking services. These services include data security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to Norway.

101. Plaintiff and Norway Subclass members were parties to such contracts, as it was their PII that Norway agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Norway Subclass members was the direct and primary objective of the contracting parties.

102. Norway knew that if it were to breach these contracts with its customers, Plaintiff and Norway Subclass members would be harmed.

103. Norway breached its contracts with customers by, among other things, failing to adequately secure Plaintiff's and Norway Subclass members' PII, and, as a result, Plaintiff and Norway Subclass members were harmed by Norway's failure to secure their PII.

104. As a direct and proximate result of Norway's breach, Plaintiff and Norway Subclass members are at a current and ongoing risk of identity theft, and Plaintiff and Norway Subclass members sustained incidental and consequential damages including: (i) financial "out of pocket"

costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to identity theft; (iv) loss of time incurred due to identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; (viii) and the continued risk of their PII, which remains in Defendants control, and which is subject to further breaches, so long as each Defendant fails to undertake appropriate or adequate measures to protect Plaintiff's and Norway Subclass members' PII.

105. Plaintiff and Norway Subclass members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT III

UNJUST ENRICHMENT (Against Norway on Behalf of the Norway Subclass)

106. Plaintiff repeats and realleges all preceding paragraphs as if fully set forth herein.

107. This count is asserted in the alternative to breach of implied contract (Count II).

108. Plaintiff and Norway Subclass members conferred a benefit on Norway with their money and data. Specifically, they engaged in banking services with Norway and in doing so also provided Norway with their PII. In exchange, Plaintiff and Norway Subclass members should have had their PII been protected with adequate data security.

109. Norway knew that Plaintiff and Class members conferred a benefit which Norway accepted. Norway profited from these transactions and used the PII of Plaintiff and Norway Subclass members for business purposes.

110. In particular, Norway enriched itself by saving the costs it reasonably should have expended on data security measures in order to secure Plaintiff's and Norway Subclass members'

PII. Instead of providing a reasonable level of security and vendor oversight that would have prevented the Data Breach, Norway instead calculated to increase its own profits at the expense of Plaintiff and Norway Subclass members by utilizing cheaper, ineffective security measures. Plaintiff and Norway Subclass members, on the other hand, suffered as a direct and proximate result of Norway's decision to prioritize its own profits over the requisite security.

111. Under the principles of equity and good conscience, Norway should not be permitted to retain the value of the PII belonging to Plaintiff and Norway Subclass members, because Norway failed to implement, and failed to ensure that its vendor Marquis implemented, appropriate data management and security measures that are mandated by industry standards.

112. Norway failed to secure Plaintiff's and Norway Subclass members' PII and, therefore, did not provide full compensation to Plaintiff and Norway Subclass members for the benefit Plaintiff and Norway Subclass members provided Norway.

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

114. Had Plaintiff and Norway Subclass members known that Norway had not reasonably secured their PII, they would not have agreed to provide their PII to Norway.

115. Plaintiff and Class members have no adequate remedy at law.

116. As a direct and proximate result of Defendants' conduct, Plaintiff and Norway Subclass members have suffered and will suffer injury, including but not limited to the following: (a) actual identity theft; (b) the loss of the opportunity to control how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and

attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Norway's possession and is subject to further unauthorized disclosures so long as Norway fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (g) 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 for the remainder of the lives of Plaintiff and Norway Subclass members.

117. As a direct and proximate result of Norway's conduct, Plaintiff and Norway Subclass members have suffered and will continue to suffer other forms of injury and/or harm.

118. Norway should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Norway Subclass members, proceeds that Norway unjustly received from them. In the alternative, Norway should be compelled to the refund to Plaintiff and Norway Subclass Members the proceeds it received because of its misconduct related to the Data Breach.

VI. PRAYER FOR RELIEF

119. WHEREFORE, Plaintiff, on his own behalf and on behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class and the Norway Subclass;

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

C. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendants' possession;

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

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

F. Such other and further relief as the Court may deem just and proper.

VII. JURY TRIAL DEMAND

120. Plaintiff hereby demands a trial by jury on all claims so triable.

DATED: November 24, 2025

Respectfully submitted,

/s/ Kelly Stewart

Kelly Stewart
Texas Bar No. 19221600
K STEWART LAW, P.C.
4597 Belfort Avenue
Dallas, Texas 75205
Telephone: (972) 308-6166
kelly@kstewartlaw.com

Israel David (*pro hac vice forthcoming*)
Adam M. Harris (*pro hac vice forthcoming*)
ISRAEL DAVID LLC
60 Broad Street, Suite 2900
New York, New York 10004
Telephone: (212) 350-8850
israel.david@davidllc.com
adam.harris@davidllc.com

Mark A. Cianci (*pro hac vice forthcoming*)
ISRAEL DAVID LLC
399 Boylston Street, Floor 6, Suite 23
Boston, MA 02116
Telephone: (617) 295-7771
mark.cianci@davidllc.com

Attorneys for Plaintiff and the Proposed Classes

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

DANIEL HART, on behalf of himself and all others similarly situated,

(b) County of Residence of First Listed Plaintiff Cumberland, Maine
(EXCEPT IN U.S. PLAINTIFF CASES)

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

K STEWART LAW, P.C., 4597 Belfort Avenue, Dallas, Texas 75205, Telephone: (972) 308-6166

DEFENDANTS

MARQUIS SOFTWARE SOLUTIONS, INC. and NORWAY SAVINGS BANK,

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

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

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

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

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

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)

Brief description of cause:
Negligence, breach of implied contract, and unjust enrichment as a result of a data breach incident.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): (Please see attached schedule of related actions)

JUDGE Amos L. Mazzant DOCKET NUMBER 4:2025cv01277

DATE Nov 25, 2025

SIGNATURE OF ATTORNEY OF RECORD /s/ Kelly Stewart

FOR OFFICE USE ONLY

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

Schedule of Related Actions

Judge	Docket No.
Chief District Judge Amos L. Mazzant	4:2025cv01277
District Judge Sean D. Jordan	4:2025cv01280
District Judge Sean D. Jordan	4:2025cv01281
District Judge Robert W. Schroeder, III	4:2025cv01284