IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS

MARQUIS SOFTWARE SOLUTIONS, INC.,	:	Civ. 4:26-cv-195
Plaintiff,	:	
v.	:	**COMPLAINT**
SONICWALL INC.,	:	
Defendant.	:	JURY TRIAL DEMANDED

Plaintiff Marquis Software Solutions, Inc. ("Marquis" or "Plaintiff"), by and through its attorneys, files this Complaint against SonicWall Inc. ("SonicWall" or "Defendant"), and alleges as follows:

SUMMARY OF THE ACTION

1. Marquis brings this lawsuit to recover the damages and losses that it has suffered from an August 2025 data incident that occurred when a threat actor easily bypassed its SonicWall firewall using credentials and configurations taken during a catastrophic data breach that SonicWall, an industry-leading cybersecurity company, experienced for several months in 2025. For a company that markets itself as an industry leader in cybersecurity and advanced network solutions, the SonicWall breach was an unprecedented failure the consequences of which are still

rippling through industry and government. The breach exposed critical security information for Marquis and every customer that used SonicWall's firewall cloud backup service, rendering those companies' networks vulnerable to targeted attack. With this breach, a national firewall provider whose job it was to protect its clients' networks, including Marquis's network, instead fully exposed them.

2. SonicWall is a cybersecurity company that markets, among other products and services, firewalls designed to protect small-to-medium businesses, enterprise customers, and federal government agencies from hackers and cybersecurity threats.

3. Plaintiff Marquis is a leader in digital marketing and compliance solutions for banks and credit unions. In 2025, Marquis began using SonicWall firewalls in its company headquarters and a company data center. Marquis purchased SonicWall firewalls based on SonicWall's reputation as an industry-leading cybersecurity company with thirty-plus years of experience and a specialty in providing cybersecurity solutions to small and medium businesses.

4. On August 14, 2025, a third-party threat actor executed a ransomware attack on Marquis, gaining unauthorized access to the company's network and client data. The impacted data included personally identifiable information concerning customers of some of Marquis's financial institution clients, information that Marquis's clients provided to Marquis to facilitate the delivery of Marquis's services.

5. Marquis took immediate steps to secure its network, notify its clients and their customers, and to investigate the incident. Over the past several months, Marquis has incurred substantial costs and damages investigating and remediating the incident, notifying impacted clients and customers, and now defending more than three dozen consumer class action lawsuits.

6. Among the questions that Marquis investigated was how the threat actor accessed its network despite the safeguards that the company had in place, including up-to-date firewalls and multi-factor authentication ("MFA"). As part of that process, it contacted SonicWall, but was ignored and denied critical information.

7. Only months later, in October 2025, did the truth begin to emerge. SonicWall had previously announced that sometime in 2025 it suffered a data breach that impacted only 5% of its customers—SonicWall assured Marquis that it was not one of them. But in October, SonicWall revealed that the data breach affecting its cloud backup service had exposed to threat actors firewall configuration files and credentials for all SonicWall customers who used the company's cloud backup service. That included Marquis.

8. In November 2025, SonicWall admitted to Marquis that the SonicWall cloud data breach had been ongoing since February 2025, when SonicWall made a code change to its application programming interface ("API") that created a vulnerability exploitable by threat actors.

9. SonicWall's cloud backup breach provided threat actors with critical data, including credentials and MFA scratch codes, that enabled them to bypass firewalls and gain access to customer networks.

10. In the case of the data incident that Marquis suffered on August 14, 2025, the previously undisclosed SonicWall cloud breach had enabled a threat actor to bypass Marquis's SonicWall firewalls despite Marquis's active MFA requirements.

11. Marquis purchased SonicWall's firewall based on their reputation and representations to create a first line of defense security system to prevent unwanted access to its internal computer systems and network by cybercriminals and cyber threats. Yet, because of SonicWall's own failures, SonicWall allowed a threat actor to obtain the keys to bypass that line of defense and walk right into Marquis's internal network, the very thing that SonicWall's firewall was supposed to prevent.

12. As a result of SonicWall's conduct, Marquis has suffered, and continues to suffer, damages; a loss of customers; harm to its business reputation; lost business opportunities, revenue and profit; and substantial diminution in its enterprise value.

PARTIES

13. Plaintiff Marquis Software Solutions, Inc. is a leader in digital marketing and compliance solutions for banks and credit unions. Marquis is a Texas corporation with its principal place of business in Plano, Texas.

14. Defendant SonicWall Inc. is a Delaware corporation with its principal place of business in Milpitas, California. SonicWall was previously owned by Dell and maintained a headquarters in Texas. Since its spinoff from Dell, SonicWall has continued to sell through Dell, including in Marquis's case, and on information and belief, maintains employees and a physical presence in Texas. SonicWall is a cybersecurity company that provides a suite of products, including firewalls, to small-to-medium businesses, enterprise customers, and federal government agencies.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(1) because this is a civil action between a citizen of Texas and a citizen of Delaware and California and the amount in controversy exceeds $75,000, exclusive of interest and costs.

16. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in Texas, has sufficient minimum contacts in Texas, and purposefully availed itself of this forum state.

17. Venue is proper in this district under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this district. Additionally, there are over thirty related class action lawsuits currently

pending in this district. *See In re Marquis Software Sols., Inc. Data Breach Litig.*, No. 4:25-cv-01277 (E.D. Tex.).

FACTUAL ALLEGATIONS

A. SonicWall

18. SonicWall is a leading cybersecurity company specializing in advanced network solutions. SonicWall describes itself as "a cybersecurity forerunner with more than 30 years of expertise [that] is recognized as a leading partner-first company."[1]

19. SonicWall offers "a full suite of solutions designed to stop targeted cyberattacks, including physical firewalls supporting deployments of all sizes, virtual firewalls, endpoint protection, email and application security, zero-trust network access, wireless security, remote workforce security, distributed network security, and more."[2]

20. SonicWall is an industry leader in cybersecurity solutions for small-to-medium businesses, but SonicWall has also expanded into the "enterprise market."[3]

---

[1] *SonicWall Report Finds Misconfigurations Driving Surging Cyberattacks in 2025*, SonicWall (Sept. 16, 2025), https://www.sonicwall.com/news/sonicwall-report-finds-misconfigurations-driving-surging-cyberattacks-in-2025.

[2] Michelle Ragusa-McBain, *Sonic Boom: Getting to Know the New SonicWall*, SonicWall (Nov. 12, 2024), https://www.sonicwall.com/blog/sonic-boom-getting-to-know-the-new-sonicwall.

[3] *Id.*

SonicWall also advertises that it provides "U.S. Government-certified cybersecurity solutions for administrative, intelligence, and military organizations and agencies," claiming that "U.S. Federal Government Agencies Trust SonicWall."[4]

21. Through its suite of network security products and services, including "expert-managed firewalls [and] advanced security services,"[5] SonicWall purports to "provide[] seamless protection against the most evasive cyberattacks across endless exposure points for increasingly remote, mobile and cloud-enabled users" and further claims that, "[w]ith its own threat research center, SonicWall can quickly and economically provide purpose-built security solutions to enable any organization—enterprise, government agencies and [small and medium-sized businesses ("SMBs")]—around the world."[6]

---

[4] *Federal Government Cybersecurity*, SonicWall, Sonicwall.com/solutions/government-federal-institutions (last visited Feb. 17, 2026).

[5] SonicWall Home Page, https://www.sonicwall.com/ (last visited Feb. 17, 2026).

[6] *SonicWall Report Finds Misconfigurations Driving Surging Cyberattacks in 2025*, SonicWall (Sept. 16, 2025), https://www.sonicwall.com/news/sonicwall-report-finds-misconfigurations-driving-surging-cyberattacks-in-2025.

22. SonicWall's website boasts various industry awards, including being named "the 2025 Security Vendor of the Year [] by D&H Distributing, a leading distributor of technology solutions to the North American channel."[7]

23. SonicWall further holds itself out as a cybersecurity expert by publishing yearly threat reports[8] and other briefings on cybersecurity threats that its products ostensibly mitigate.

24. SonicWall represents that it is "a 100% channel-driven company," meaning that it sells its products to end users through partners.[9]

B. SonicWall's Firewall Products

25. SonicWall calls itself "a pioneer of firewall technology" that "offers firewall models for businesses of every size."[10] SonicWall claims that its firewall models provide "[b]est-in-class [t]hreat [p]rotection," "[e]nterprise-grade

---

[7] *SonicWall Named a "Vendor of the Year' by D&H Distributing*, SonicWall (Dec. 16, 2025), https://www.sonicwall.com/news/sonicwall-named-a-vendor-of-the-year-by-d-h-distributing; *see also* https://www.sonicwall.com/about-sonicwall/awards

[8] *See Security News & Threat Intelligence*, SonicWall, https://www.sonicwall.com/threat-report (last visited Feb. 17, 2026).

[9] Michelle Ragusa-McBain, *Sonic Boom: Getting to Know the New SonicWall*, SonicWall (Nov. 12, 2024), https://www.sonicwall.com/blog/sonic-boom-getting-to-know-the-new-sonicwall.

[10] *Network Security Firewalls*, SonicWall, https://www.sonicwall.com/products/firewalls (last visited Feb. 17, 2026).

protection," and "[u]nrivaled threat protection," that its "firewalls deliver proven security, performance, and simplicity for modern networks," and that they are "[d]esigned for stronger protection, easier management, and long-term resilience as threats evolve."[11]

26. A firewall is "[a] device or program that controls the flow of network traffic between networks or hosts" in order to "prevent unauthorized accesses to or from a private network."[12] Put differently, "[a] firewall around a computer or network is like the wall around a castle or city. It protects the computer or network by limiting points of access and providing criteria that must be met before being allowed to enter."[13]

27. SonicWall markets a line of "Next Generation Firewalls" ("NGFW"), marketing different series models based on business size. SonicWall describes its TZ Series firewalls as "[e]nterprise-grade protection for your small to mid-size business or branch office." SonicWall markets its NS*a* series firewalls to "mid-sized

---

[11] *Id.*

[12] *Firewall*, Nat'l Inst. Standards & Tech., https://csrc.nist.gov/glossary/term/firewall (last visited Feb. 17, 2026).

[13] *How Firewalls Work*, Bos. Univ. TechWeb, https://www.bu.edu/tech/about/security-resources/host-based/intro/ (last visited Feb. 17, 2026).

enterprises," claiming that they offer "[u]nrivaled threat prevention in a high-performance security platform."[14]

28. SonicWall claims that "[t]he SonicWall TZ series of firewalls is designed specifically for the needs of SMBs and branch locations, delivering enterprise-class security without the enterprise-grade complexity," and that TZ Series firewalls "[p]rotect your small business or branch location from intrusion, malware and ransomware with an easy-to-use, integrated security solution designed specifically for your needs."[15]

29. SonicWall claims that its "Network Security appliance (NS*a*) Mid-Range Firewall protects against day-to-day incursions and advanced threats like ransomware, attacks against non-standard ports, and breaches in firewalls, all at the speed of business. With cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, secure SD-WAN,

---

[14] *Network Security Firewalls*, SonicWall, https://www.sonicwall.com/products/firewalls (last visited Feb. 17, 2026).

[15] *Introducing Gen 8 TZ Series Next-Generation Firewall (NGFW)*, SonicWall, https://www.sonicwall.com/products/firewalls/entry-level (last visited Feb. 17, 2026).

real-time visualization, and WLAN management, SonicWall provides flexible, fast, and cost-effective security to keep the threats out and your business thriving."[16]

30. SonicWall also offered its firewall customers the ability to create cloud backups of their firewalls through the MySonicWall cloud service. This allowed customers to securely store, manage, and retrieve firewall configuration files.

C. Marquis's Deployment of SonicWall Firewalls

31. In 2025, Marquis deployed SonicWall Firewalls in both its corporate headquarters and a company data center.

32. Marquis deployed TZ series firewalls in its Plano, TX headquarters.

33. In April 2025, Marquis purchased a SonicWall NS*a* series firewall device for a company data center through Dell Technologies. Marquis's purchase included SonicWall remote implementation and premier support services.

34. Prior to the August 14, 2025 incident, Marquis had implemented comprehensive security measures on its SonicWall firewalls, with MFA enabled from the outset. The firewalls were protected by MFA on all administrative accounts with complex passwords, and the SonicWall admin interface was locked down with a limited allow list. Marquis further implemented the full suite of managed security

[16] *Introducing Gen 8 NS*a *Series Next-Generation Firewall (NGFW)*, SonicWall https://www.sonicwall.com/products/firewalls/mid-range (last visited Feb. 17, 2026).

features, including gateway services, content filtering, botnet filtering, and geo-blocking, and had configured all accounts with Active Directory and MFA.

D. The August 2025 Data Incident

35. On August 14, 2025, Marquis detected unusual activity on its network. Marquis took immediate steps to secure its network, isolate the intrusion, and launch a thorough investigation.

36. Marquis determined that a third-party threat actor had gained unauthorized access to its network and to certain client data.

37. The attack on Marquis was a ransomware attack. A ransomware attack is where a threat actor utilizes a type of malware to encrypt a victim's data where the attacker demands a "ransom," or payment, in order to restore access to files and network.

38. On the day of the August 14, 2025 incident, Marquis opened a ticket with SonicWall support to investigate the cause and ensure it was protected. SonicWall support subsequently instructed Marquis that, for security-specific information related to the event, Marquis would have to submit a form to SonicWall's Product Security Incident Response Team ("PSIRT"). Marquis submitted the form as instructed and followed up with its SonicWall account team on multiple occasions, but never received a response from Sonicwall's PSIRT. In the aftermath of the incident, Marquis continued to contact SonicWall but was repeatedly denied critical information.

39. Because of the quick actions and steps that Marquis took to protect its network and client information, Marquis is still not aware of any evidence of actual or attempted misuse of personal information as a result of the incident.

40. Marquis immediately began notifying affected clients of the incident, and over the next few months worked hand-in-hand with its clients to notify consumers whose PII might have been accessed by the threat actor.

41. As part of its response to the incident, Marquis examined the potential root cause or attack vector that the threat actor had utilized to gain access to Marquis's network. After an investigation, Marquis determined that there was no known unpatched vulnerability in its SonicWall firewalls that could have explained the threat actor's ability to bypass Marquis's first line defenses and access the company's network.

E. The MySonicWall Cloud Backup Breach

42. For its firewall customers, SonicWall offered a "cloud backup" service, through which SonicWall stored its customers' backup firewall configurations. The cloud backup service was a feature where firewalls would automatically upload configuration backups to SonicWall's cloud infrastructure. The backups were stored in an S3 bucket on Amazon's infrastructure, maintained by SonicWall. The primary purpose of this service was to provide customers with off-site backup copies of their firewall configurations, allowing them to recover settings in case of device failure

or the need to migrate configurations to new hardware. These backup files could be used and imported to another platform.

43. From at least February 2025 through September 2025, a threat actor gained unauthorized access to SonicWall customers' backup firewall configurations by exploiting a vulnerability that SonicWall had introduced through a code change to its API in February 2025.

44. SonicWall failed to detect the cloud backup breach for several months. SonicWall has represented publicly that it first detected suspicious activity related to the downloading of backup firewall configuration files stored in its cloud environment in early September 2025.[17]

45. On September 17, 2025, SonicWall publicly announced a security breach affecting customers with MySonicWall cloud backups. That same day, SonicWall revised its incident disclosure to "clarify" the "scope" of the incident, publicly representing that the breach had affected "<5% of firewalls."[18]

---

[17] *Cloud Backup Security Incident Investigation Complete and Strengthened Cyber Resilience*, SonicWall (Nov. 4, 2025), https://www.sonicwall.com/blog/cloud-backup-security-incident-investigation-complete-and-strengthened-cyber-resilience.

[18] *MySonicWall Cloud Backup File Incident*, SonicWall (updated Oct. 28, 2025), https://www.sonicwall.com/support/notices/mysonicwall-cloud-backup-file-incident/kA1VN0000000RoD0AU.

46. SonicWall advised its customers to take certain remedial actions in response to SonicWall's security breach, and also encouraged customers to log into their MySonicWall accounts to verify whether their firewall devices were at risk.

47. Following SonicWall's instructions, Marquis logged into its MySonicWall account and ran the serial numbers of its firewall devices. Marquis observed that SonicWall had not flagged Marquis's devices as having been impacted by the SonicWall Breach. A SonicWall Premier Services support representative confirmed via email that, if Marquis's serial numbers were not flagged, then the company "should be fine." Nevertheless, and in an abundance of caution, Marquis immediately took the remedial steps that SonicWall had outlined in its disclosure.

48. On October 8, 2025, SonicWall updated its incident disclosure to reveal that its incident response firm, Mandiant, had completed its investigation and "confirmed that an unauthorized party [had] accessed firewall configuration backup files for all customers who have used SonicWall's cloud backup service."[19] SonicWall acknowledged that the compromised files had included "encrypted

[19] In a YouTube video released on October 15, 2025, SonicWall admitted that the erroneous assessment that the cloud breach had impacted fewer than 5% of firewalls was SonicWall's initial assessment, and that Mandiant determined the breach was far more widespread after conducting its own investigation. *See* SonicWall, *Important SonicWall Cloud Backup Security Update - 10-13-25*, at 2:00, 3:36-4:58 (YouTube, Oct. 15, 2025), https://www.youtube.com/watch?v=GxKzkkSYKAE.

credentials and configuration data," and that "while encryption remains in place, possession of these files could increase the risk of targeted attacks."[20]

49. The configuration backups that the SonicWall breach compromised contained numerous pieces of sensitive data that could be leveraged to facilitate an attack against SonicWall users. SonicWall has admitted publicly and privately that the information could include unencrypted MFA scratch codes, unencrypted usernames, SSL certificate information, local firewall and linked customer domain encrypted username passwords, firewall rules, and overall configuration information. As one industry source reported, the backups that SonicWall exposed "contained sensitive configuration data such as network rules, VPN setups, credentials, and certificates," data that,"[i]n the wrong hands, . . . provides valuable insight into internal networks and could help attackers plan targeted intrusions."[21]

---

[20] *MySonicWall Cloud Backup File Incident*, SonicWall (updated Oct. 28, 2025), https://www.sonicwall.com/support/notices/mysonicwall-cloud-backup-file-incident/kA1VN0000000RoD0AU; *see also MySonicWall Cloud Backup Data Breach*, Beazley Security, https://beazley.security/alerts-advisories/mysonicwall-cloud-backup-data-breach (last visited Feb. 18, 2026) ("SonicWall determined that the MySonicWall cloud backup environment was compromised, which allowed attackers unauthorized access to configuration backups from every customer utilizing the service." (emphasis omitted)).

[21] *See, e.g.*, Sascha Hasse, *When Trust Becomes a Threat: The SonicWall Breach and the Case for Zero Trust Security*, Wire (Oct. 10, 2025), https://wire.com/en/blog/sonicwall-breach-zero-trust.

50. Unfortunately for Marquis, SonicWall's discovery and warnings regarding its own breach and the risks it created were too late. When Marquis learned that SonicWall's representations from September 2025 were incorrect, and that the SonicWall Breach had in fact impacted Marquis's firewall devices, Marquis—in an abundance of caution—completed SonicWall's recommended remediation a second time.

51. Following this corrected disclosure, Marquis also sought additional information from SonicWall regarding the SonicWall Breach. During subsequent conversations, a SonicWall executive confirmed that Marquis's firewall backup was downloaded during the SonicWall Breach and that the breach had exposed everything in Marquis's firewall, including credentials and MFA scratch codes.

52. SonicWall also disclosed to Marquis that the SonicWall cloud breach had been ongoing for several months before SonicWall discovered the intrusion. Though SonicWall has stated publicly that it first detected unusual activity in September 2025, a SonicWall executive relayed to Marquis that SonicWall had begun investigating in August 2025, when attacks on its customers had begun, but that SonicWall later determined that the malicious activity traced to February 2025.

53. Regarding the root cause of the SonicWall cloud breach, the SonicWall representative explained that SonicWall had made a code change to its API in February 2025 that had introduced a vulnerability allowing threat actors to access

configuration backup files from every customer using the company's cloud backup service without proper authentication. Specifically, the vulnerability allowed anyone with a device serial number, which can be generated by algorithm and are generally predictable, to download the configuration backups without using any SonicWall credentials. As a self-proclaimed cybersecurity forerunner, SonicWall had reason to know that using predictable device serial numbers created a foreseeable vulnerability that threat actors could—and did—easily exploit. SonicWall's reckless use of easy-to-predict, easy-to-brute-force serial numbers constitutes a marked failure to implement reasonable and appropriate security measures to prevent unauthorized disclosure of its customers' protected data.

54. When Marquis asked SonicWall representatives how the threat actor that attacked Marquis could have accessed Marquis's network even though Marquis had enabled MFA, the SonicWall executive attributed it to SonicWall's cloud breach. The SonicWall representatives explained that SonicWall's biggest concern following the SonicWall Breach was the bypassing of two-factor authentication that customers had set up on their systems. Shockingly, the representatives explained that the SonicWall cloud breach had made this possible because SonicWall had stored customer MFA scratch codes within the configuration backup files without encrypting them.

55. MFA scratch codes within the stolen configurations could be used to bypass MFA requirements in customer firewalls. MFA scratch codes are one-time-use codes to bypass MFA in the event of an emergency where the user may not be able to access their dual-factor authentication device or application. Exposure of MFA scratch codes poses a clear and substantial risk to a company using MFA in conjunction with its SonicWall firewall. SonicWall's failure to encrypt the scratch codes is an egregious departure from the normal standard of care expected of a company in SonicWall's position.

56. During these conversations, SonicWall disclosed that its PSIRT team had reviewed evidence related to the Marquis attack and determined that the attack scenario fit the parameters of what SonicWall had seen with other customers who were suffering attacks as a result of SonicWall's cloud backup breach. Specifically, SonicWall's PSIRT team indicated that the way the threat actor had entered Marquis's network and perimeter defenses was consistent with what SonicWall was seeing with other attacks caused by the SonicWall cloud breach.

57. As a result of SonicWall's gross negligence in introducing a vulnerability into its cloud backup service, in failing to detect a months-long intrusion, failing to properly warn and protect Marquis and other customers, and in failing to properly encrypt customer configuration data, including MFA scratch

codes, SonicWall directly and proximately caused attacks on its customers' networks, including Marquis's, which have resulted in substantial financial damage.

F. Harm to Marquis and Its Clients

58. The SonicWall Breach has created astounding financial repercussions for Marquis. These costs have included, but are not limited to, legal costs and costs associated with the ransom demand, the forensic investigation, breach notifications, and remediations. In addition to these costs, Marquis has suffered significant commercial and reputational harm as a direct result of the SonicWall Breach.

59. Marquis has incurred substantial costs and fees, including attorney's fees, (a) investigating and remediating the August 14, 2025 incident; (b) disclosing the incident to its clients; (c) assessing the impact of the incident on client data; (d) assisting its clients in providing required notifications to their customers and members; and (e) offering credit monitoring services to impacted consumers.

60. Marquis has also been named as a defendant in dozens of putative class actions (the "Related Actions"), which seek millions of dollars in damages in relation to the August 14, 2025 incident. (*See* Exhibit A). It is also facing one commercial lawsuit, in which a customer asserts a misappropriation of trade secrets claim resulting from the Marquis incident. *See New Orleans Firemen's Fed. Credit Union v. Marquis Software Sols., Inc.*, No. 4:26-cv-00037 (E.D. Tex. Jan. 13, 2026). In addition to the potential damages from these lawsuits, Marquis has incurred, and will continue to incur, substantial legal costs in defending these cases. SonicWall has not

yet been named as a defendant in the Related Actions or any other actions related the SonicWall Breach.

61. Commercially, the SonicWall Breach has cost Marquis both existing and new business opportunities. Marquis clients have terminated their contracts with Marquis prematurely, refusing to pay amounts owed under their agreements and in some cases seeking return of fees prepaid to Marquis.

62. The SonicWall breach has also harmed Marquis reputationally. As a result of the breach, a national trade association refused to allow Marquis to continue serving as a lead sponsor of an important industry conference and, for a time, even disinvited Marquis from the conference altogether. Marquis has been forced to expend time, resources, and money to affirmatively defend its actions in front of its existing customers.

63. Marquis's clients have also incurred costs and fees in connection with notifying their impacted customers and members. Some Marquis clients have in turn demanded that Marquis reimburse the clients for costs and fees associated with notifying the clients' impacted customers and members.

G. SonicWall Failed to Adequately Safeguard Customers' Data

64. As the SonicWall cloud backup breach shows, Defendant SonicWall did not use reasonable security measures appropriate to the sensitive firewall data that it collected from customers like Marquis and stored in its cloud environment.

65. A number of published industry and national best practices are widely used as a go-to resource when developing an institution's cybersecurity standards.

66. For example, the National Institute of Standards and Technology ("NIST") recommends certain practices to safeguard systems, such as controlling who logs into your network and encrypting sensitive data, at rest and in transit.

67. Similarly, the Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cyberattacks, including (a) ensuring privileged or administrative access requires MFA; and (b) taking steps to quickly detect a potential intrusion, including "ensur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior."[22]

68. Similarly, Microsoft's Threat Protection Intelligence Team recommends that companies monitor for adversarial activities, hunt for brute force attempts, monitor for cleanup of event logs, and analyze logon events.

69. It was reasonable for SonicWall customers like Marquis to believe that a cybersecurity company with three decades of experience that marketed itself as an expert in cybersecurity, firewalls, and advanced network solutions, would employ industry standard and reasonable security measures to protect its network

---

[22] *Shields Up: Guidance for Organizations*, CISA, https://www.cisa.gov/shields-guidance-organizations (last visited Feb. 18, 2026).

environment and customer data, particularly extremely sensitive data related to customer firewall configurations.

70. In reality, SonicWall (a) introduced a vulnerability into its own cloud service, (b) failed to detect an intrusion that ran for months in which a threat actor gained access to firewall configuration data for every SonicWall customer that used the company's cloud service, (c) stored Marquis's critical data (e.g., MFA scratch codes) that would enable threat actors to bypass critical perimeter defenses on customer networks in an unencrypted format, and (d) failed to adequately and timely respond to inquiries by Marquis to allow it to prevent, remediate, and investigate the effects of the data breach.

71. SonicWall has refused to correct its wrongs, including refusing to indemnify Marquis.

COUNT ONE
(Negligence)

72. Plaintiff repeats and realleges paragraphs 1 through 71 hereof, as if fully set forth herein.

73. By providing Marquis with firewall and cloud backup services, SonicWall undertook a duty to use reasonable care in providing those services.

74. Moreover, SonicWall's sole business purpose is to provide services such as those it promised to provide to Marquis, and SonicWall holds itself out as an expert in providing such services.

75. As alleged herein, SonicWall breached its duties by failing to act in accordance with a minimum standard of care in allowing a threat actor to gain access to Marquis's firewall configuration data and, thereby, facilitating a threat actor's unauthorized access to Marquis's network and to Marquis's client's data.

76. SonicWall further breached its duties by failing to detect the vulnerability for several months after it had exposed Marquis's firewall configuration data.

77. Specifically, SonicWall breached the duty that it owed to Marquis by, among other things:

a. Failing to properly monitor its network for unauthorized access by threat actors;

b. Failing to prohibit unauthorized access to its network;

c. Failing to take the proper and necessary precautions in monitoring its network;

d. Failing to perform its services in a good and safe manner;

e. Causing or allowing dangerous conditions as a result of its failure to properly monitor its network;

f. Failing to appropriately recognize the risk of a cybersecurity infiltration and elevate the threat assessment accordingly;

g. Failing to train and/or supervise its employees, contractors, subcontractors, or agents acting under SonicWall's direction to properly monitor its network; and

h. Other acts and omissions as discovery may reveal.

78. As a direct, proximate, and foreseeable result of SonicWall's negligence, Plaintiff Marquis has suffered damages, including investigation and remediation costs, the cost of notifying Marquis's clients, consumers, and regulators regarding the data incident, the cost of providing credit monitoring products, loss of sales, lost revenue, loss of business reputation, and loss of goodwill.

COUNT TWO
(Gross Negligence)

79. Plaintiff repeats and realleges paragraphs 1 through 78 hereof, as if fully set forth herein.

80. By providing Marquis with a firewall and cloud backup services, SonicWall undertook a duty to use reasonable care to avoid causing foreseeable risk of injury to Marquis in providing those services.

81. As alleged herein, SonicWall breached its duties by allowing a threat actor to gain access to Marquis's firewall configuration data and, thereby, facilitating

a threat actor's unauthorized access to Marquis's network and to Marquis's client's data.

82. SonicWall's breach was an extreme departure from the ordinary standard of care and gross negligence in that SonicWall, a cybersecurity company whose commercial purpose was to protect its customers' networks, including by selling and servicing firewalls, stored copies of its customers' firewall configuration data in the cloud, failed to encrypt critical components of that data, made a coding change that introduced a vulnerability into its cloud service that was exploitable for unauthorized access, failed to notice for more than six months that all its customers' firewall configurations were exposed to threat actors, and then falsely represented to customers for weeks that the breach had impacted fewer than 5% of firewalls, when the incident had in fact exposed firewall configuration data for every customer that used SonicWall's cloud backup service.

83. Specifically, SonicWall recklessly disregarded the rights of Marquis by:

a. Failing to properly monitor its network for unauthorized access by threat actors;

b. Failing to prohibit unauthorized access to its network;

c. Failing to take the proper and necessary precautions in monitoring its network;

d. Failing to perform its services in a good and safe manner;

e. Causing or allowing dangerous conditions as a result of its failure to properly monitor its network;

f. Failing to appropriately recognize the risk of a cybersecurity infiltration and elevate the threat assessment accordingly;

g. Failing to train and/or supervise its employees, contractors, subcontractors, or agents acting under SonicWall's direction to properly monitor its network; and

h. Other acts and omissions as discovery may reveal.

84. As a direct, proximate, and foreseeable result of SonicWall's gross negligence and recklessness, Plaintiff Marquis has suffered damages, including investigation and remediation costs, the cost of notifying Marquis's clients, consumers, and regulators regarding the data incident, the cost of providing credit monitoring products, loss of sales, lost revenue, loss of business reputation, and loss of goodwill.

COUNT THREE
(Unjust Enrichment)

85. Plaintiff repeats and realleges paragraphs 1 through 84 hereof, as if fully set forth herein.

86. Plaintiff Marquis conferred a benefit upon Defendant by purchasing firewall hardware, support services, and implementation services from SonicWall.

87. Plaintiff Marquis also conferred a benefit upon Defendant by expending its own time, resources, and money to remediate and investigate the data incident caused by the SonicWall cloud backup breach, to notify impacted clients and consumers, as well as regulators, and to defend litigation arising from the data incident, costs that, legally and rightfully, were SonicWall's to bear given that the SonicWall cloud backup breach was a direct and proximate cause of the data incident that Marquis experienced on August 14, 2025.

88. Plaintiff Marquis has demanded that SonicWall indemnify and reimburse Marquis for the costs, fees, expenses, and damages that Marquis has incurred as a result of the SonicWall cloud backup breach, which SonicWall has wrongfully refused to do.

89. Defendant SonicWall has accepted and enjoyed the aforementioned benefits, knowing that Marquis had conferred those benefits, without any objection or notice of any defects.

90. Under principles of equity and good conscience, SonicWall should not be permitted to retain the full value of Plaintiff's payments, and should be required to reimburse the costs, fees, and damages Marquis has incurred as a result of the SonicWall cloud backup breach, because SonicWall failed to adequately safeguard Marquis's network, firewall devices, and firewall configuration data, and Marquis would not have conferred these benefits upon SonicWall had it known that

SonicWall would not adequately safeguard Marquis's network, firewall devices, and firewall configuration data.

91. Defendant SonicWall should be required to disgorge all unlawful or inequitable proceeds received and/or retained by it because of its misconduct and the data breach and associated harm that it has caused.

COUNT FOUR
(Negligent Misrepresentation)

92. Plaintiff repeats and realleges paragraphs 1 through 91 hereof, as if fully set forth herein.

93. As discussed above, Marquis purchased firewall devices, premier support services, and remote implementation services from SonicWall to fortify Marquis's network against potential cyberattacks.

94. SonicWall has made material misrepresentations and/or omissions concerning the performance of its firewalls and the safety, security, and performance of its cloud backup service, with the intent of inducing small-to-medium businesses like Marquis to purchase SonicWall products and services.

95. SonicWall failed to exercise reasonable care in making said representations about the performance, safety, and security of its products and services, including its cloud backup service.

96. Marquis reasonably relied upon SonicWall's material misrepresentations and/or omissions during the course of its relationship with SonicWall, to its detriment.

97. As a direct, proximate, and foreseeable result of SonicWall's negligent misrepresentations, Plaintiff Marquis has suffered damages, including investigation and remediation costs, the cost of notifying Marquis's clients, consumers, and regulators regarding the data incident, the cost of providing credit monitoring products, loss of sales, lost revenue, loss of business reputation, and loss of goodwill.

COUNT FIVE
(Contribution)

98. Plaintiff repeats and realleges paragraphs 1 through 97 hereof, as if fully set forth herein.

99. Marquis faces the possibility of a judgment rendered against it in the Related Actions, for which claimants seek recovery of damages for the exposure of their PII in the August 2025 Marquis data incident.

100. Any losses suffered by Plaintiffs in the Related Actions were the direct result of SonicWall's own negligence.

101. Among other things, SonicWall's own, unnoticed network vulnerabilities allowed a threat actor to gain access to Marquis's firewall configuration data and, thereby, facilitated a threat actor's unauthorized access to

Marquis's network and to Marquis's client's data, including the PII of the plaintiffs in the Related Actions.

102. Plaintiffs in the Related Actions seek no relief from SonicWall.

103. Marquis is entitled to contribution from SonicWall up to the percentage of responsibility which SonicWall bears in connection with any damages awarded to the plaintiffs in the Related Actions against SonicWall.

COUNT SIX
(Common Law Indemnity)

104. Plaintiff repeats and realleges paragraphs 1 through 103 hereof, as if fully set forth herein.

105. If and to the extent that plaintiffs in the Related Actions establish liability against Marquis (which liability Marquis expressly denies), any losses suffered by plaintiffs in the Related Actions were the direct result of SonicWall's negligence.

106. Among other things, SonicWall's own, unnoticed network vulnerabilities allowed a threat actor to gain access to Marquis's firewall configuration data and, thereby, facilitated a threat actor's unauthorized access to Marquis's network and to Marquis's client's data, including the PII of the plaintiffs in the Related Actions.

107. Marquis is entitled to full equitable indemnity from SonicWall, including reimbursement of any judgment payments made on behalf of Marquis and

recovery of attorneys' fees and costs in defending against the Related Actions and in pursuing this claim.

108. In the alternative, Marquis is entitled to partial equitable indemnity from SonicWall for any monetary sums that Marquis is required to pay plaintiffs in the Related Actions in excess of Marquis's proportionate share of liability.

PRAYER FOR RELIEF

WHEREFORE, as a result of the foregoing, Marquis demands judgment in its favor and against SonicWall as follows:

A. Awarding damages, including for investigation and remediation costs, the cost of notifying Marquis's clients, consumers, and regulators regarding the data incident, the cost of providing credit monitoring products, defense of the related lawsuits, loss of sales, lost revenue, lost profits, loss of business reputation, and loss of goodwill, and as described in each of the above claims, in favor of Marquis and against SonicWall, in an amount to be established according to proof at trial;

B. Awarding Marquis pre- and post-judgment interest, attorney's fees and costs, and other expenses occurred in this action;

C. Awarding Marquis injunctive and other equitable relief as necessary to protect Marquis's interests; and

D. Granting Marquis such further relief as may be just and proper.

[SIGNATURE PAGE FOLLOWS]

Dated: February 23, 2026

Respectfully submitted,

By: */s/ Melissa R. Smith*

Melissa R. Smith
Texas State Bar No. 24001351
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Phone: (903) 934-8450
Fax: (903) 934-9257
melissa@gillamsmithlaw.com

W. Kyle Tayman (*admission pending*)
Jordan L. Moran
D.C. Bar Number 888273537
GOODWIN PROCTER LLP
1900 N Street NW
Washington, DC 20036
Phone: (202) 346-4000
Fax: (202) 346-4444
KTayman@goodwinlaw.com
JordanMoran@goodwinlaw.com

Attorneys for Plaintiff
MARQUIS SOFTWARE SOLUTIONS, INC.

EXHIBIT A

Below is a list of putative class action complaints currently pending against Marquis:

- *In re Marquis Software Solutions, Inc. Data Breach Litigation*, No. 4:25-cv-01277 (E.D. Tex.) (consisting of 33 consolidated class action complaints)
- *Yunk v. Covantage Credit Union*, No. 4:26-cv-00108 (E.D. Tex.)
- *Bellissimo v. Marquis Software Solutions, Inc.*, No. 4:26-cv-00169 (E.D. Tex.)