UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

IN RE: SONIC CORP. CUSTOMER DATA SECURITY BREACH LITIGATION (FINANCIAL INSTITUTIONS)	CASE NO. 1:17-md-2807 MDL No. 2807 ORDER [Resolving Doc. 431; Doc. 395; Doc. 311]

JAMES S. GWIN, UNITED STATES DISTRICT JUDGE:

In 2017, unidentified third parties accessed Sonic[1] customers' payment card data. The hackers stole customer payment card information from more than seven-hundred Sonic franchised Drive-Ins.

The compromised Sonic Drive-In restaurants were independently owned, but Sonic's franchise agreements required the franchisees give Sonic access to the franchisees' transaction data through a Sonic-managed virtual private network (VPN).[2] The hackers accessed the franchisees' transaction data using VPN credentials that Sonic had issued to a transaction-processing service.

In this case, Plaintiff financial institutions sue Defendants for negligence in creating unsecure systems that led to the breach. The Court certified a class action.[3]

Defendants now seek summary judgment.[4] After reviewing the parties' extensive

[1] Sonic Corporation and its subsidiaries and affiliates Sonic Industries Services, Inc., Sonic Capital LLC, Sonic Franchising LLC, Sonic Industries LLC, and Sonic Restaurants, Inc. (collectively, "Sonic" or "Sonic Defendants" or "Defendants").

[2] Doc. 437-5 at 7, 16, 18 (Sonic Franchising LLC License Agreement); Doc. 435-1 at ¶ 17 (Davis Declaration).

[3] Doc. 343; Doc. 348.

[4] Doc 431; Doc. 431-1. Over the course of the year, the parties have filed multiple versions of their summary judgment related documents. For ease and clarity, the Court cites the final versions.

briefing, the Court finds that genuine fact questions remain. Defendant fails to show sufficient support for summary judgment.

For the following reasons, the Court **DENIES** Defendants' summary judgment motion.

I. Background

The underlying facts in this case have not changed since the Court ruled on the motion to dismiss: Between April and October 2017, hackers used malware installed on point-of-sale systems at 762 Sonic-branded restaurants to steal sales transaction payment card data.[5] The hackers targeted Sonic franchises that used an Infor-brand point-of-sale system.

Although franchisees were independently owned and operated, Sonic set the parameters for transaction processing. Sonic required all franchisees to process all credit card transactions through First Data Merchant Services.[6] Franchisees used point-of-sale vendors, including Infor, for transaction-processing services that interfaced with First Data.[7]

Sonic stores used two types of transaction-processing systems: the POPS system at drive-in stalls, and the PAYS system at the drive-through window and inside the restaurant.[8] The hack occurred in the PAYS system.[9]

---

[5] Doc. 202 at 5.

[6] Doc. 431-1 at 7.

[7] *Id.* at 8.

[8] Doc. 431-1 at 7.

[9] Doc. 435-1 at ¶ 36 (Davis Declaration); Doc. 437-2 at 14 (Trustwave Report).

Here and elsewhere, the Court cites a report by Trustwave, a third party Sonic engaged to conduct a forensic investigation following the breach. Doc. 437-2 at 8. This report is likely admissible under Federal Rule of Evidence 801(d)(2)(D), as an admission by an agent. *See Beck v. Haik*, 377 F.3d 624, 639-40 (6th Cir. 2004), *overruled on other grounds by Adkins v. Wolever*, 554 F.3d 650, 651 (6th Cir. 2009) (holding that an outside risk consultant is an "agent" for the purposes of this rule).

Alternatively, it may be admissible as an authorized admission under Rule 801(d)(2)(C) or a business record under Rule 803(6). *Marceau v. Int'l Bhd. of Elec. Workers*, 618 F. Supp. 2d 1127, 1142-43 (D. Ariz. 2009); *Northgate Lincoln-Mercury Inc. v. Ford Motor Co.*, 507 F. Supp. 3d 940, 952 (S.D. Ohio 2020).

Regardless of admissibility, the Court may properly consider this evidence at the summary judgment

The un-hacked POPS system encrypts customer data end-to-end.[10] The hacked PAYS system, instead, allowed unencrypted data to remain on franchisee servers.[11] The VPN system allowed the hackers to access that unencrypted customer payment card data.

While the parties disagree about the extent of Sonic corporate's involvement with franchisee technology systems, both recognize a significant ongoing Sonic role.

Point-of-sale vendors like Infor process the transactions, but "the general infrastructure of the PAYS environment is designed by Sonic."[12] Sonic also facilitates the VPN that vendors use to access franchise systems remotely.[13] As the Sonic Defendants acknowledge, "Sonic corporate assisted its franchisees in setting up a dedicated VPN solution" for Infor to provide remote service assistance.[14] As part of this assistance, Sonic issued credentials to Infor to access the Sonic VPN.[15]

The hackers—likely German-based—used the Infor credentials to access the Sonic-created VPN channel.[16] For more than six months, the hackers were able to steal payment card data without detection.[17]

Multiple factors facilitated the hackers' access to the Sonic VPN. Sonic left Infor's remote access to the VPN "permanently enabled," meaning that a hacker who obtained the Infor credential could connect to the VPN at any time.[18] At the time of the breach, Sonic

---

stage. *Bethel v. Jenkins*, 988 F.3d 931, 938 (6th Cir. 2021).

[10] Doc. 435-1 at ¶ 12 (Davis Declaration).

[11] Doc. 437-2 at 14 (Trustwave Report); Doc. 437-17 at 52-54 (Ernst & Young Report). The Ernst & Young report is likely admissible for the same reasons as the Trustwave report.

[12] Doc. 435-2 at ¶ 20 (Simon Declaration).

[13] Doc. 437-2 at 14 (Trustwave Report).

[14] Doc. 431-1 at 10-11.

[15] Doc. 433 at 17:12-14, 18:22, 30:24; Doc. 437-2 at 14.

[16] Doc. 431-1 at 12; Doc. 436 at 5; *see also* Doc. 437-14.

[17] Doc 437-2 at 8-9, 17 (Trustwave Report).

[18] Doc. 431-1 at 11; Doc. 437-2 at 17 (Trustwave Report).

had not yet introduced a centralized logging system to monitor or alert for malicious activity.[19] Outdated software and weak passwords for both the Sonic-issued credential and the Infor servers also contributed to the breach.[20]

The parties dispute whether Sonic or Infor was responsible for logging and monitoring VPN access, changing the password for the Sonic-issued credential, and making the necessary changes to update the software.[21] Material facts remain unresolved.

II. Discussion

a. Summary Judgment Standard

A party should receive summary judgment if "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law."[22] A genuine issue of material fact exists where "a reasonable jury could return a verdict for the nonmoving party" based on the evidence.[23]

In reviewing a motion for summary judgment, the Court views all evidence in the light most favorable to the nonmoving party.[24] The nonmoving party "must show sufficient evidence to create a genuine issue of material fact"[25] as to each of the claim's required elements.[26] But summary judgment is still appropriate "[i]f the evidence is merely colorable

---

[19] Doc. 437-2 at 17 (Trustwave Report).

[20] *Id.*

[21] Doc. 431-1 at 17; Doc. 436 at 19-20.

[22] *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986) (citation omitted).

[23] *Peffer v. Stephens*, 880 F.3d 256, 262 (6th Cir. 2018) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)).

[24] *Thomas v. Speedway SuperAmerica, LLC*, 506 F.3d 496, 500–01 (6th Cir. 2007) (citation omitted).

[25] *Id.* (citation omitted).

[26] *Id.* (noting that a scintilla of evidence is not enough to defeat a summary judgment motion).

. . . or is not significantly probative."[27]

b. Defendants' Summary Judgment Motion

After the Court partially granted Defendants' motion to dismiss, only Plaintiffs' negligence claim remains.[28]

Under Oklahoma law, a negligence claim requires that (1) Defendants owed Plaintiffs a duty of care; (2) Defendants breached their duty; and (3) Defendants' breach caused Plaintiffs' injury.[29]

Defendants argue that the Court should grant their motion for summary judgment because Plaintiffs' claim fails on the duty and causation requirements. Viewing the facts in a light most favorable to Plaintiff, the Court disagrees.

i. Duty

Defendants contend that they did not owe Plaintiffs a duty to prevent the data breach.

Under Oklahoma law, except in certain circumstances, Defendants do not have a duty to "anticipate and prevent the intentional or criminal acts of a third party."[30] Under Oklahoma law, Sonic Defendants owe Plaintiffs a duty if the Sonic Defendants' "own *affirmative* act has created or exposed [Plaintiffs] to a recognizable high degree of risk of harm through such misconduct, which a reasonable [person] would have taken into account."[31]

---

[27] *Liberty Lobby, Inc.*, 477 U.S. at 249-50.

[28] *See* Doc. 304 at 6–11.

[29] *Lowery v. Echostar Satellite Corp.*, 160 P.3d 959, 964 (Okla. 2007).

[30] *BancFirst v. Dixie Restaurants, Inc.*, No. CIV-11-174-L, 2012 WL 12879, at *3-4 (W.D. Okla. Jan. 4, 2012) (citing *J.S. v. Harris*, 227 P.3d 1089, 1092–94 (Okla. Ct. App. 2009)).

[31] *J.S. v. Harris*, 227 P.3d at 1092 (Okla. Ct. App. 2009) (citing *Joyce v. M & M Gas Co.*, 672 P.2d 1172, 1174 (Okla. 1983)).

"Whether a duty exists is a threshold legal question for the court."[32]

Sonic Defendants say that Plaintiffs have not and cannot show that Defendants' affirmative acts created a risk of harm from a data breach.[33] Defendants blame Infor, the point-of-sale system vendor, for creating the data breach harm through its acts and systems.[34]

The Court disagrees with Defendants' argument. Sonic had a duty to prevent the criminal acts of hackers because Sonic's affirmative acts created a risk of harm, and Sonic knew or should have known that the risk of hacking made its flawed security practices unreasonably dangerous.

1. Affirmative Acts

Sonic committed multiple affirmative acts exposing Plaintiffs to a high degree of risk.

At the very least, the parties agree on two key Sonic actions: "(1) that Sonic created a permanently-enabled VPN tunnel that did not block foreign IP addresses" that gave Infor—and anyone with Infor's credentials—access to each Infor-served franchise point-of-sale systems and "(2) that Sonic created, for Infor's use in remotely accessing the VPN tunnel, the remote user credential 'infor_nrowan' without multi-factor authentication enabled."[35]

The evidence, viewed in the light most favorable to Plaintiffs, also suggests two additional affirmative acts by Sonic Defendants. First, Sonic required franchisees to use middleware that did not support point-to-point encryption. In addition, Sonic controlled middleware upgrades, and caused delays that left franchisees operating vulnerable systems.

Sonic developed and controlled the PAYS and POPS payment systems and required

---

[32] *McGehee v. Forest Oil Corp.*, 908 F.3d 619, 624 (10th Cir. 2018) (citing Oklahoma law).
[33] Doc. 434 at 15.
[34] *Id.* at 16.
[35] *Id.* at 7–8.

franchisees to process transactions through the PAYS or POPS systems.[36] Sonic Defendants also created and, to some extent, managed the VPN tunnel that the hackers used to access the franchisee customer's payment card data. [37]

The parties present competing evidence on the extent to which the affected point-of-sale systems were protected by end-to-end or point-to-point encryption.[38] A forensic report concluded that in the PAYS system, data was encrypted at the time of payment but decrypted during processing.[39] Other evidence also suggests that the WinEPS 828 middleware transaction processing software did not allow end-to-end encryption.[40]

At the July 28, 2021 hearing, Sonic's counsel suggested that franchisees' systems had some point-to-point encryption.[41] Likely true. Sonic did not use the vulnerable WinEPS 828 payment system with the POPS payment system.[42] Defendants' briefs do not explain, however, how Infor could encrypt from end to end while using the WinEPS 828 payment system.

Sufficient evidence also supports Plaintiffs' argument that Sonic's delays in introducing new versions of WinEPS affected Infor's ability to transition to newer versions of the middleware software.[43] OpenEPS, a replacement for WinEPS 828, supports end-to-end

---

[36] Doc. 431-1 at 7; *see also* Doc. 437-5 at 7, 9, 16 (Sonic Franchising LLC License Agreement).

[37] Doc. 434 at 7. Defendants admit: "Sonic corporate assisted its franchisees in setting up a dedicated VPN solution for Infor's exclusive use to permit Infor to remotely access the Infor POS Systems in order to push updates, service the systems, or troubleshoot any problems, for example." Doc. 431-1 at 22.

[38] Doc. 436 at 25-26.

[39] Doc. 437-2 at 14 (Trustwave Report).

[40] Doc. 437-17 at 52-54 (Ernst & Young Report).

[41] Doc. 433 at 15:17-20.

[42] *Id.* at 26:18.

[43] For example, when introduced in 2014, WinEPS 828 was incompatible with Infor's payment terminals. Doc. 437-7 at 2 (email from Sonic employee adopting statement by Infor employee). Infor informed Sonic of this problem in 2014, but Sonic did not solve the issue until 2016. *Id.* While waiting for Sonic to solve the compatibility problem, Infor needed to use an older version of the software, WinEPS 825. *Id.*

encryption but Sonic did not make it available to Infor PAYS users before the data breach.[44]

Viewing the evidence in the light most favorable to Plaintiffs, Sonic required franchisees to use middleware transaction processing software that did not allow end-to-end encryption of payment card data. In doing so, Sonic precipitated the franchisees storing unencrypted transaction data on the franchisees' servers.[45] The hackers then stole this unencrypted transaction data.

Sonic's actions were affirmative acts creating a foreseeable risk of harm.

2. Recognizable Risk of Harm

Under Oklahoma law, not every defendant action that creates a foreseeable risk of harm creates a duty.[46] Rather, the question is whether a defendant "knew or should have known" of the risk of harm that made a defendant's actions "unreasonably dangerous."[47]

Sonic knew or should have known the risks in requiring franchisees to use a system with a permanently enabled access point protected only by a weak password, no point-to-point encryption, and outdated software. Sonic also should have recognized the risks in requiring franchisees to use a system that provided access without effective logging or log monitoring.[48]

The Sonic Defendants were aware of and concerned about hacking risks. Sonic was

---

[44] Doc. 437-7 at 2 (email from Sonic employee adopting statement by Infor employee); Doc. 437-31 at 2 (email from Sonic employee); Doc. 437-46 at 2 (emails from Sonic employees); Doc. 437-50 at 5 (Sonic presentation).

[45] Doc. 437-2 at 14 (Trustwave Report): "At each location transactions occur either through a POPS environment, which is end-to-end encrypted, . . . or through a PAYS environment . . . Infor PAYS environment data is encrypted in transit between the terminal and radio server but decrypted at the radio server or the BoH system depending on the hardware in use at each location."

[46] *McGehee*, 908 F.3d at 625–626.

[47] *Id.* at 625, 628 (citing *Lowery*, 160 P.3d at 964–65).

[48] *See* Doc. 437-2 at 17-18 (Trustwave Report).

aware of other similar breaches.[49] Sonic Defendants knew the danger of cybersecurity breaches and had given cybersecurity-related management and guidance to franchisees.[50]

In sum, Sonic Defendants created risks through multiple affirmative acts despite awareness of the risks. Defendants' affirmative actions created the opportunity for foreseeable harm when they created an insecure access point for Infor. Sonic knew or should have known that the Sonic-issued credentials providing access to the VPN were vulnerable to attack because they had no multifactor authentication and only a minimally complex password requirement. Defendants were aware of the risk of a hack as they had elsewhere taken different steps to protect themselves, consumers, and financial institutions. Finally, Sonic should have known the dangers in creating such a vulnerable access point to a system containing unencrypted credit card data.[51]

Given these facts, Defendants' actions were "unreasonably dangerous." Defendants owed Plaintiffs a duty.

ii. Causation

Defendants also argue their actions did not proximately cause the data breach.[52] To Defendants, creating the VPN tunnel and providing Infor with hackable, non-multifactor credentials were not actions that caused the breach.[53] Defendants instead argue that the hackers' breach and data theft acted as supervening causes that cut off Defendants' liability.[54]

---

[49] *See, e.g.*, Doc. 437-14.
[50] *See, e.g.*, Doc. 437-9; Doc. 437-10.
[51] Doc. 437-17 at 52-54 (Ernst & Young Report).
[52] Doc. 432 at 4.
[53] *Id.*
[54] *Id.* at 7.

Proximate cause is typically a jury fact question.[55] Proximate cause is appropriate for summary judgment as a legal question only where "the evidence together with all inferences which may be properly deduced therefrom is insufficient to show a causal connection between the alleged wrong and the injury."[56]

Further, in Oklahoma,

> [f]or an intervenor's act to become a "*supervening cause*" and cut off possible liability for the original negligence, it must (1) be independent of the primary negligence, (2) be adequate *of itself* to bring about the injury complained of and (3) not be a reasonably foreseeable event. When such an act qualifies as a *supervening cause*, the original negligence mutates into a mere *condition* and as a matter of law is no longer actionable. When, however, the intervening act is a *reasonably foreseeable consequence* of the primary negligence, the original wrongdoer will not be relieved of liability. Also, where the primary act of negligence is not superseded by a second cause—*i.e.*, continues to operate concurrently, so that damage is the result of both causes acting in concert—each act may be regarded as the proximate cause and the wrongdoers will be jointly and severally liable for the plaintiff's compensable harm.[57]

Here, Sonic can only prevail by showing that the hackers' criminal acts were independent of Sonic's negligent security practices, that these criminal acts were adequate of themselves to bring about the hack, *and* that the hack was not a reasonably foreseeable event. Questions of material fact block Sonic-favorable findings on each of these three conclusions.

Sonic's role in creating the numerous and distinct vulnerabilities that separately contributed to Plaintiffs' claimed injuries is a sufficiently disputed material fact. Sonic

[55] *Lockhart v. Loosen*, 943 P.2d 1074, 1079–80 (Okla. 1997).
[56] *Id.* at 1080 (citing *Smith v. Davis,* 430 P.2d 799, 800 (Okla.1967)).
[57] *Id.* at 1079 (emphasis in original).

inexplicably gave Infor access to over 760 Sonic franchisees' payment systems without requiring dual authentication.[58] Sonic never required periodic password change nor required any minimal level of password complexity.[59] Sonic never limited foreign access to the VPN and never established a useful logging system tied to alerts.[60] Also, Sonic arguably used a middleware transaction processing software that could not accommodate end-to-end encryption.[61] Sonic disputes its responsibility for these problems but presents insufficient evidence to now resolve these questions.

A reasonably jury could find that the hack was a foreseeable consequence of creating and maintaining a vulnerable entry point. Without the vulnerable Sonic-created access point, the hackers would not have been able to breach the affected restaurants' point-of-sale systems and steal card information. The failure to provide PAYS payment processing software that Infor could encrypt made card compromise foreseeable. The failure to limit access to domestic users and the failure to log and alert suspicious activity, made a greater card member loss foreseeable.

Also, Sonic's creation of a credential with permanently enabled access to the VPN tunnel made the damage worse. The harm from the vulnerable VPN channel "continue[d] to operate concurrently" because the hack was able to continue as long as the VPN remained accessible. Rather than a single-event intrusion, the Sonic hackers used the VPN credential for more than six months to mine more and more franchisees' data.[62]

---

[58] Doc. 436 at 5, 23-24.
[59] *Id.* at 22-23; *see also* Doc. 437-2 at 17 (Trustwave Report).
[60] Doc. 436 at 16, 22; *see also* Doc. 437-2 at 17-18, 47-48 (Trustwave Report).
[61] Doc. 436 at 25-26.
[62] Doc 437-2 at 8-9, 17 (Trustwave Report).

Sufficient evidence also supports an argument that, independent of the VPN failure, end-to-end encryption would have stopped the damage. Independent of the VPN failure, blocks on foreign users would have stopped the damage. Independent of the VPN failure, logging and alerts would have reduced the damage. Sonic fails to show that the hackers' acts superseded Sonic's acts.

Further, even if Sonic Defendants had never experienced a data breach in this way, many other retail companies had suffered similar data breaches. That is why Sonic's other VPN credentials used multifactor authentication.[63] And that is why Sonic documents nominally *required* "external support personnel" to use multifactor authentication.[64] Indeed, Sonic's actions addressing the hack underscore the importance of this security measure. Once Sonic enabled multifactor authentication for the "infor_nrowan" credential, the hackers lost access to customer card data.[65]

On this record, a reasonable jury could find that the hack was not an independent cause of the Plaintiffs' injury. Arguably, Plaintiffs needed to reissue cards and reimburse fraudulent charges because customers' card data was stolen in a data breach made possible because Sonic created a vulnerable entry point.

There is sufficient evidence that Sonic Defendants' actions were the proximate cause of Plaintiffs' injury to make summary judgment inappropriate. Proximate cause is a question for the trier of fact in this case.

[63] Doc. 433 at 18:15–19:3.
[64] Doc. 437-14.
[65] Doc. 437-2 at 9, 18 (Trustwave Report).

II. Conclusion

For the foregoing reasons, the Court **DENIES** Defendants' summary judgment motion.

ITS IS SO ORDERED.

Dated: September 7, 2021

s/ James S. Gwin
JAMES S. GWIN
UNITED STATES DISTRICT JUDGE