

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
NORTHEASTERN DIVISION**

GEMSTONE FOODS, LLC et al.,)
)
Plaintiffs,)
)
v.)
)
AAA FOODS ENTERPRISES, INC.)
et al.,)
)
Defendants.)
)

Case No.: 5:15-cv-02207-MHH

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
NORTHEASTERN DIVISION**

MICHAEL ENSLEY et al.,)
)
Plaintiffs,)
)
v.)
)
BEN O. TURNAGE et al.,)
)
Defendants.)
)

Case No.: 5:15-cv-01179-MHH

MEMORANDUM OPINION – VOLUME V

Computer Fraud and Abuse Act

Gemstone and RCF allege that the defendants violated the Computer Fraud and Abuse Act – the CFAA – because the defendants “retained possession of a laptop computer through which Defendants accessed Plaintiffs’ information from a

protected computer used in interstate commerce and communication. Defendants lacked authority and/or exceeded their authority to access this information.” (Doc. 391, pp. 89–90, ¶ 5.132). “Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer” violates the CFAA. 18 U.S.C. § 1030(a)(2)(C). “[E]xceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). The CFAA provides a private right of action for “[a]ny person who suffers damage or loss by reason of a violation of [the CFAA].” 18 U.S.C. § 1030(g).

Gemstone’s CFAA claim pertains to the Wester laptop. (Doc. 391, pp. 89–90). Mr. Wester accessed Gemstone information from the Toshiba laptop while he worked for Gemstone and after he left Gemstone and brought the laptop to Farm Fresh. Mr. Wester may be liable to Gemstone under the CFAA if, when he used the laptop to access Gemstone information, he obtained Gemstone information that he was not authorized to obtain.

The Supreme Court’s recent decision in *Van Buren v. United States*, 141 S. Ct. 1648 (2021), sheds light on Gemstone’s claim concerning the Wester laptop. In *Van Buren*, the defendant, a former police sergeant, “used his patrol-car computer to access the law enforcement database with his valid credentials” to run a license-

plate search in exchange for money. *Van Buren*, 141 S. Ct. at 1653. The United States charged the police officer with a felony violation of the CFAA “on the ground that running the license plate . . . violated the ‘exceeds authorized access’ clause of 18 U.S.C. § 1030(a)(2).” *Van Buren*, 141 S. Ct. at 1653. The jury convicted the defendant, and the Eleventh Circuit affirmed the conviction, finding that the police officer exceeded his authorized access under the CFAA because, although he had the technological ability, permission, and credentials to access his computer and retrieve license plate information, he “access[ed] the law enforcement database for an ‘inappropriate reason.’” *Van Buren*, 141 S. Ct. at 1654.

The Supreme Court granted certiorari in *Van Buren* to examine potential CFAA liability for people who access computers they are authorized to access, obtain information on those computers they are authorized to obtain, but then use that information for an improper purpose. *See Van Buren*, 141 S. Ct. at 1653 n.2. The Supreme Court found that such people do not violate the CFAA:

In sum, an individual “exceeds authorized access” when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him. The parties agree that [the defendant] accessed the law enforcement database system with authorization. The only question is whether [the defendant] could use the system to retrieve license-plate information. Both sides agree that he could. [The defendant] accordingly did not “excee[d] authorized access” to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose. We therefore reverse the contrary judgment of the Eleventh Circuit

Van Buren, 141 S. Ct. at 1662.

Under *Van Buren* then, the dispositive question is whether Mr. Wester was restricted from accessing Gemstone's computer system from the Toshiba laptop, restricted from accessing policy documents and other records that he copied, and/or restricted from accessing co-employees' email accounts and email messages which he did not receive through his own Gemstone email account. Viewing the evidence in the light most favorable to Gemstone and RCF, the answer is yes and no. The parties seem to agree that, while Mr. Wester worked at Gemstone, he was authorized to access policy documents and other records from Gemstone's computer system.¹ Therefore, a CFAA claim may not rest on evidence that Mr. Wester downloaded to the Toshiba laptop certain Gemstone forms and policies while he worked at Gemstone.

The Gemstone employee email accounts that Mr. Wester accessed in the Gemstone computer system and downloaded onto the laptop are another matter. In his first deposition, Mr. Wester testified that when Gemstone began operating, he helped employees set up their email accounts. (Doc. 422-8, p. 14, tpp. 50–51). He stated that when Gemstone opened its second plant, he set up a Gmail account in his

¹ Again, Mr. Wester began as the shipping manager at Gemstone and later became responsible for quality assurance. (Doc. 422-8, p. 9, tp. 31). Jurors reasonably could infer that he had access to employee policies and various Gemstone forms used in shipping and used for purposes of quality assurance.

name so that “[they] could access files at either plant one or plant two.” (Doc. 422-8, pp. 18–19, tpp. 68–69; *see also* Doc. 422-8, p. 19, tp. 70). At some point while he was working at Gemstone, Mr. Wester loaded his co-employees’ Gemstone email accounts onto the Toshiba laptop. In his first deposition, Mr. Wester testified that in 2014, he would backup the laptop monthly because Mr. Welborn, Mr. Pass, and Ms. Campos “kept losing” email messages. (Doc. 422-8, p. 23, tpp. 87–88). Mr. Wester acknowledged that he created several accounts on the laptop for Gemstone employees, including Mr. Power and Mr. Knight, in January and February of 2015 after discussions about the creation of Farm Fresh were underway. (Doc. 422-8, pp. 25–26, tpp. 96–98). Mr. Wester stated that he was “keeping everybody updated.” (Doc. 422-8, p. 26, tp. 97). In addition, Mr. Wester acknowledged that after he left Gemstone on February 16, 2015, he continued to set up Gemstone email accounts on the laptop. (Doc. 422-8, pp. 26–27, tpp. 98–102).

Mr. Wester was not authorized to access Gemstone’s computer system and take information from Gemstone email accounts after he left Gemstone. Mr. Wester’s technological ability to access the email accounts because Gemstone had not yet changed the passwords for the accounts is not the equivalent of permission to access the accounts. Jurors reasonably could conclude from the evidence that Gemstone did not learn that Mr. Wester took the Toshiba laptop with him when he left the company until Mr. Wester turned the laptop over to his attorneys in 2018,

and Gemstone did not know that Mr. Wester had downloaded Gemstone employees' email accounts onto the laptop until a forensic examination of the laptop was completed during this litigation. Unlike the parties in the *Van Buren* case, the parties here do not agree that Mr. Wester was authorized to access Gemstone email accounts after he left Gemstone. In fact, there is no evidence in the record that indicates that Gemstone gave Mr. Wester permission to access Gemstone email accounts after he left the company in February of 2015.

Moreover, the evidence viewed in the light most favorable to the plaintiffs indicates that, even while he worked at Gemstone, Mr. Wester did not have permission to access Gemstone email accounts other than his own. Mr. Wicker testified that he was responsible for setting up employees' email accounts. (Doc. 419-7, p. 13, tp. 40).² Mr. Wicker testified that Mr. Wester did not inform him that he (Mr. Wester) was setting up Outlook email accounts as a backup in case Gemstone employees lost email messages. (Doc. 419-7, p. 53, tp. 200). When asked in his deposition whether he authorized Mr. Wester to place his Gemstone email account on the Toshiba laptop, Mr. Welborn said no. (Doc. 419-9, p. 27, tpp. 101–

² Mr. Pass testified that he believed that Mr. Wicker would set up new email accounts, pass the information on to Mr. Wester, and Mr. Wester would set up the accounts on Gemstone computers. (Doc. 422-6, p. 26, tp. 98). Mr. Wicker explained that when he created email accounts for new employees, he would send the employees a temporary password with an instruction to change the password when they first logged into their accounts. (Doc. 419-7, p. 13, tp. 41). Mr. Wicker testified that someone else became responsible for administering Gemstone email accounts in 2015. (Doc. 419-7, p. 55, tp. 206). Mr. Power testified that when he joined Gemstone in November of 2014, Kevin Wilson set up his Gemstone email account. (Doc. 422-12, p. 84, tp. 323).

02). Mr. Pass did not remember Mr. Wester informing him (Mr. Pass) that his email would be downloaded onto the Toshiba laptop. (Doc. 422-6, p. 26, tpp. 97–98). Mr. Power and Mr. Easterling testified that they did not know of anyone at Gemstone who had access to their Gemstone Foods Outlook accounts while they worked for the company. (Doc. 422-10, p. 70, tp. 266; Doc. 422-12, p. 84, tp. 324). And in his first deposition, Mr. Wester testified that neither Mr. Ensley nor Gary Hill knew that he (Mr. Wester) had installed co-employees’ Gemstone email accounts on the Toshiba laptop. (Doc. 422-8, p. 26–27, 100–01). The Court has found no evidence, other than Mr. Wester’s testimony, that suggests that Gemstone gave him ongoing access to Gemstone email accounts other than his own. A jury does not have to accept Mr. Wester’s testimony in this regard.³ Therefore, evidence concerning a CFAA violation connected to Wester laptop is disputed.

³ The evidence shows that, while he was working at Gemstone, Mr. Wester accessed confidential email messages on which he was not copied and shared those messages with his co-defendants in this action. (Doc. 454-28, p. 79 (confidential email message indicating that Gemstone planned to replace Mr. Welborn); Doc. 422-4, p. 18, tp. 65 (Mr. Welborn’s testimony that Mr. Wester “brought [him] a hard copy of an email where . . . they [were] going to hire somebody half [his] age and half [his] salary”)). There is no evidence that indicates that someone at Gemstone authorized Mr. Wester to access confidential messages that were not addressed to him. Under *Van Buren*, if Mr. Wester was not authorized to access the email accounts, then his taking and distributing confidential messages likely violates the CFAA. Sharing the confidential email messages with his co-defendant may be only an “improper purpose” if Mr. Wester had permission to access the email accounts from which he took the messages, but *Van Buren* does not speak directly to the question of whether a document or email designated as confidential limits a defendant’s general authorized access to, for example, email accounts.

Before a jury may decide whether Mr. Wester violated the CFAA, Gemstone must identify evidence of damages the company incurred because of the alleged CFAA violation. A party may proceed with a civil action for a CFAA violation only if the alleged misconduct involves one of several factors, including “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i)(I). A CFAA “loss” is “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). Damages under this subsection are limited to economic damages. 18 U.S.C. § 1030(g). The Eleventh Circuit has held:

The plain language of the statutory definition includes two separate types of loss: (1) reasonable costs incurred in connection with such activities as responding to a violation, assessing the damage done, and restoring the affected data, program system, or information to its condition prior to the violation; and (2) any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. . . . “Loss” includes the direct costs of responding to the violation in the first portion of the definition, and consequential damages resulting from interruption of service in the second.

Brown Jordan Int’l, Inc. v. Carmicle, 846 F.3d 1167, 1174 (11th Cir. 2017).

In *Brown Jordan*, the defendant repeatedly accessed the email accounts of other employees and his supervisors by using a generic password that was identical

for all accounts, and he took screenshots of hundreds of emails over the course of six months. *Brown Jordan*, 846 F.3d at 1171. Brown Jordan argued that it incurred loss because it paid an “outside consultant, Crowe Horwath, to assess how [the defendant] accessed the emails, and [paid] a contractor, Kroll, to sweep the office building for audio and video surveillance devices.” *Brown Jordan*, 846 F.3d at 1172. After a bench trial, the district court concluded that the defendant’s actions violated the CFAA, and the Eleventh Circuit affirmed. The Eleventh Circuit noted that the “losses were incurred in the course of responding to the offense and are therefore compensable under the CFAA,” and clarified that the reasonable cost of responding to unauthorized email access “is not limited to damage to a computer or network.” *Brown Jordan*, 846 F.3d at 1174–75 & n.2.

Gemstone asserted in its third amended complaint that “Plaintiffs have suffered damages far greater than the \$5,000 threshold stated in the CFAA as a result of this illegal conduct.” (Doc. 391, p. 90, ¶ 5.132). In its response to Mr. Wester’s summary judgment motion, Gemstone stated that CFAA “violations caused or contributed to significant damage to Plaintiffs as Defendants took advantage of Plaintiffs’ information and employed it against them.” (Doc. 454, p. 67). Several district courts in the Eleventh Circuit have held that ““allegations that [a defendant] attempted to enter into new business ventures with [a plaintiff’s] clients by using stolen trade secrets are insufficient to demonstrate ‘loss’ ”” under the CFAA. *My*

Energy Monster, Inc. v. Gawrych, No. 8:20-cv-2548-MSS-AEP, 2021 WL 6125579, at *3 (M.D. Fla. Sept. 29, 2021) (quoting *Fla. Beauty Flora Inc. v. Pro Intermodal L.L.C.*, No. 20-20966-CIV-ALTONAGA/Goodman, 2020 WL 4003494, at *7 (S.D. Fla. July 15, 2020) and collecting other cases). And Gemstone has not alleged that Mr. Wester’s unauthorized email access caused an “interruption of service.” Therefore, Gemstone can establish a CFAA loss only if the company can prove that it incurred costs in response to Mr. Wester’s allegedly unauthorized email access. See *St. Johns Vein Ctr., Inc. v. StreamlineMD LLC*, 347 F. Supp. 3d 1047, 1060 (M.D. Fla. 2018); see also *Brown Jordan*, 846 F.3d at 1174.

Hiring a forensic analyst to investigate the extent of unauthorized email access is a loss “incurred in the course of responding to the offense” and therefore is cognizable under the CFAA. See *Brown Jordan*, 846 F.3d at 1174–75; *My Energy Monster, Inc.*, 2021 WL 6125579, at *4; *Hall v. Sargeant*, No. 18-80748-CIV-ALTMAN/Reinhart, 2020 WL 1536435, at *32 (S.D. Fla. Mar. 30, 2020). The expert report prepared by Dr. Gavin Manes indicates that he was “retained by [Gemstone’s law firm] to perform work on behalf of their client Gemstone, LLC. Specifically, [he] was asked to review the forensics image of a laptop.” (Doc. 454-28, p. 2, ¶ 9). Dr. Manes testified that he was contacted about the Wester laptop shortly after it was disclosed, (Doc. 419-10, p. 11, tp. 9); the defendants disclosed the laptop to Gemstone on August 3, 2018, (Doc. 159, p. 2). Most of Dr. Manes’s

investigation was completed over the summer of 2020 after the parties spent the better part of one year negotiating a protocol for examining the laptop. (Doc. 419-10, p. 12, tp. 10; *see, e.g.*, Doc. 201). The “original goal” regarding the Wester laptop was “to determine if there was [sic] documents that [they] could directly relate to Gemstone on the laptop.” (Doc. 419-10, p. 14, tp. 12).

Importantly, Gemstone did not have an opportunity to investigate the extent of its loss related to the Wester laptop until Mr. Wester came forward with the laptop during this litigation. Gemstone’s investigation necessarily was tied to discovery in this litigation because of the timing of Mr. Wester’s disclosure, and the delayed start to the investigation was the consequence of this highly-contested litigation, not foot-dragging on Gemstone’s part. Reasonable jurors could conclude that Dr. Manes examined the laptop solely for this litigation. But reasonable jurors also could conclude that Dr. Manes’s work served two purposes: his work enabled Gemstone to develop trial evidence and to determine the extent of Mr. Wester’s unauthorized access to Gemstone information via Gemstone’s computer system and assess necessary corrective measures. Because the Court must draw inferences from the evidence in favor of the non-moving party, the Court determines that the cost of conducting a forensic analysis of the Wester laptop may be considered a cost

incurred in response to the alleged CFAA violation.⁴ *Compare Sartori v. Schrodt*, 424 F. Supp. 3d 1121, 1130 n.9 (N.D. Fla. 2019) (“Obviously, the money that [the plaintiff] spent to hire a computer expert to substantiate this civil action is not a ‘loss’ contemplated by the statute.”); *Hamilton Grp. Funding, Inc. v. Basel*, No. 16-61145-CIV-ZLOCH, 2019 WL 3765340, at *4–5 (S.D. Fla. Aug. 7, 2019) (collecting cases allowing recovery of attorney fees for a CFAA violation but distinguishing them from the attorney fees at issue in *Basel* because the work done was “too remote” from the CFAA violation). Therefore, Gemstone’s CFAA claim shall proceed, but even if a jury finds a CFAA violation, Gemstone will not be able to recover damages unless a jury also determines that Gemstone suffered a loss of at least \$5,000.

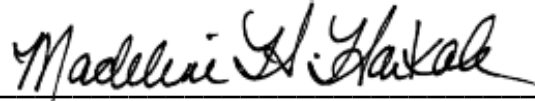
In sum, Gemstone’s CFAA claim against Mr. Wester concerning email accounts on the Toshiba laptop survives the defendants’ summary judgment motion. The Court will grant the defendants’ motion for summary judgment as it pertains to Gemstone documents that Mr. Wester copied before he left the company.⁵

⁴ Dr. Manes charged just under \$20,000 for his work. (Doc. 454-28, p. 3, ¶ 14). Gemstone may recover charges assessed within the span of one year under § 1030(g).

⁵ To the extent that the CFAA claim extends to defendants like Gary Hill who copied Gemstone documents shortly before they left Gemstone, no evidence suggests that the defendants did not have access to those documents, (Doc. 422-8, p. 28, tp. 107), so for the same reason that a CFAA claim as to those documents fails against Mr. Wester, the claim also fails as to other defendants.

As the CFAA claim pertains to use of the Toshiba laptop by defendants other than Mr. Wester, viewed in the light most favorable to the plaintiffs, the evidence suggests that defendants other than Mr. Wester used the laptop after the laptop arrived at Farm Fresh. In his first deposition, Mr. Wester testified that after he left Gemstone in early 2015, he gave the Toshiba laptop to Gary Hill at Mr. Ensley’s direction. (Doc. 422-8, pp. 20, 22–23, tpp. 74–75, 84–85). Somehow, the laptop

DONE and **ORDERED** this February 26, 2022.



MADELINE HUGHES HAIKALA
UNITED STATES DISTRICT JUDGE

ended up in the shipping department at Farm Fresh, and the laptop was used there periodically. But there is no evidence that a defendant other than Mr. Wester downloaded Gemstone emails and proprietary information onto the laptop after the laptop arrived at Farm Fresh. Because the evidence in this respect is not developed sufficiently for jurors to base a decision on facts rather than speculation, the Court will grant the motion for summary judgment on the CFAA claim as to all defendants other than Mr. Wester.