Question MPT-2 – July 2024 – Selected Answer 1

Breen & Lennon LLP
520 Jackson Blvd.
Bristol, Franklin 33708

MEMORANDUM

TO: Damien Breen
FROM: Examinee
DATE: July 30, 2024
RE: Sidecar Design matter

Introduction

Earlier, you asked me to determine whether our client Sidecar Design ("Sidecar") is liable to CDI under the federal Computer Fraud and Abuse Act ("CFAA") and, if Sidecar is liable, what damages it owes to CDI under the CFAA.

In brief, Sidecar is likely not liable for the $25,000 transfer made prior to the end of the contract because there was no technological or legal restraint on Sidecar's ability to access CDI's data. However, it is likely liable for the $50,000 transfer made after the end of the contract because there was a legal restraint on Sidecar's ability to access CDI's data. If Sidecar is liable, CDI can recover only $5,500 because its consequential damages do not arise out of an interruption in services and no punitive damages are available under CFAA.

Analysis

I. Sidecar Design is likely not liable for the transfer made prior to the end of the contract because there was no technological or legal restraint on access, but is likely liable for the transfer made after the end of the contract because there was a legal restraint on access.

A person is liable under the CFAA if it knowingly and with intent to defraud (1) either accesses a computer without authorization or exceeds its authorized access; and (2) by means of such conduct, furthers the intended fraud and obtains anything of value. 18 U.S.C. Sec. 1030(a)(4). The CFFA applies all computers connected to the Internet. *Van Buren v. U.S.* (U.S. 2021).

A person exceeds his authorized access if he accesses a computer with authorization and uses such access to obtain or alter information in the computer that he is not entitled to obtain or alter. 18 U.S.C. Sec. 1030(e)(6). The Supreme Court has held that a person exceeds his authorized access when he accesses data that the person does not have the technical right to access. *Van Buren*. The Supreme Court has clarified that a mere organizational policy that restricts a member's access is not, by itself, sufficient to make that member's access to a computer unauthorized, if there are no technical restraints on the member's ability to access the computer. *Id.*; *see also HomeFresh LLC v. Amity Supply Inc.* (D. Frank. 2022) (an employer's policy forbidding an employee from accessing customer information did not make the employee's access unauthorized because the employee was able to access customer information using his employee credentials). While *Van Buren* is a criminal case, the CFAA has been interpreted to apply uniformly across civil and criminal cases. *Homefresh* (citing U.S. v. Nosal (9th Cir. 2012)).

The *Van Buren* court did not address whether a legal restraint on access is sufficient to make a person's access to a computer unauthorized. A Franklin District Court has held that a legal restraint arising from contract on a person's ability to access a computer is so sufficient. *HomeFresh*. Thus, access of a company computer by a former employee is considered unauthorized access under the CFAA, even if the former employee is using previously authorized and unaltered credentials. *Id.* However, other Circuits have found that such legal restraints are not sufficient to make access unauthorized. *See id.* (discussing the approach of other Circuits).

In this situation, the perpetrator of the fraud, John Smith ("Smith"), was employed as a software engineer at Sidecar. During the contract period between Sidecar and CDI, CDI provided Sidecar with a password that gave Sidecar full access to all the data in CDI's system, including customer payment information. The password also enabled Sidecar to alter the deposit account to which customer bills would be paid. Nothing in the contract itself appears to have provided a legal restraint on Sidecar's authority to access data. Therefore, during the contract period, there was neither a technological nor a legal restraint on Sidecars authority to access and alter data. Therefore, Smith's access to and alteration of customer data was not unauthorized under the CFAA. *Van Buren*; *HomeFresh*. The mere presence of CDI's "repeated insistence" that Sidecar create a password-protected system for customer information and that Sidecar not used customer data is not enough to make Smith's technologically and legally unfettered access to and use of that data unauthorized. *Van Buren*; *HomeFresh*. Therefore, Sidecar is not liable for Smith's transfer of $25,000 prior to the end of the contract term.

However, Sidecar is likely liable for Smith's transfers after the end of the contract term. *HomeFresh*. Because Sidecar's legal authority to access CDI's data ended after the contract term, Smith's access to CDI's data after the contract ended is likely unauthorized. *Id.* Smith's actions are much like the defendant's agent in *HomeFresh*. There, the agent used his unaltered previously authorized credentials to access a company's computer after the agent had left the company. *Id.* Because the agent no longer had legal authority to access the company computer, as he had left the company, the Franklin District Court found the agent's access to be unauthorized under CFAA, even though there were no technological barriers to the agent's access. In this case, there were no technological barriers to Smith's access to CDI's data because CDI failed to change its password. However, once Sidecar's contract with CDI had ended, Sidecar no longer had legal authority to access CDI's data. Therefore, Smith's access to CDI's data would, under *HomeFresh*, be considered unauthorized under the CFAA. Therefore, Sidecar is likely liable for Smith's $50,000 after Sidecar's contract with CDI had ended. However, while *HomeFresh* heavily supports this conclusion, it was made only by a District Court, and the 15th Circuit has not yet determined whether a legal restraint on access is alone sufficient to make a person's access to a computer unauthorized.

In conclusion, Sidecar is likely not liable for Smith's $25,000 transfer made prior to the end of Sidecar's contract with CDI, but Sidecar is likely liable for Smith's $50,00 0 transfer made prior to the end of the contract.

II. If Sidecar is liable, CDI can likely recover

A victim of a violation of the CFAA is generally entitled to obtain consequential damages resulting from that conduct. 18 U.S.C. Sec. 1030(g). However, the victim may only recover for losses if they exceed a threshold amount of $5,000 during any one-year period, and any such damages for a violation are limited to economic damages. *Id.*

A loss includes any reasonable cost to a victim, including the costs of response, conducting a damage assessment, and restoring things to their condition prior to the offense. 18 U.S.C. Sec. 1030(e)(11). The victim of hacking cannot claim improvements to security or a system as losses. *Slalom Supply v. Bonilla* (15th Cir. 2023). But external cybersecurity investigation costs and internal employee time spent to remedy a violation is recoverable. *Id.*

The CFAA also limits compensable losses to only those that result specifically from an interruption in service due to a violation of the CFAA. *Id.*; *Cyranos Inc. v. Lollard* (D. Frank. 2017) (permitting damages for lost revenue when an outage resulting from the violation occurred during a period of peak sales business). Thus, "lost revenues and consequential damages qualify as losses only when the plaintiff experiences an interruption in service." *Selvage Pharm. v. George* (D. Frank. 2018) (emphasis added). This typically occurs if a violation results in the loss of something that results in the loss of a lucrative business opportunity or the alteration of system-wide passwords. *See Ridley Mfg. v. Chang* (D. Frank. 2015); *Marx Florals v. Teft* (D. Frank. 2012).

The CFAA precludes punitive damages. *Demidoff v. Park* (15th. Cir. 2014).

CDI may recover the $4,000 it was charged by an outside cybersecurity firm to investigate and fix the breach. *Bonilla.* It may also recover the $1,500 CDI spent on overtime for its employees to help with the cybersecurity firm's investigation. *Id.* However, it cannot recover for the $500 CDI spent to upgrade its security system. *Id.* Because CDI's qualifying losses exceed $5,000 in a given year, it may bring suit.

CDI cannot recover for the pending contract to CDI worth $125,000, because the loss of that business opportunity is not tied to the interruption of service suffered by CDI as result of Smith's violation of the CFAA. *Id.* For similar reasons, CDI could not recover the $75,000 in transferred funds, just as the plaintiff in *Bonilla* could not recover in restitution, as these losses did not occur as a result of an interruption in service. *Id.* CDI could recover only for any business or revenue lost as a result of its website being shut down for five days to investigate and fix the breach. *Id.* CDI cannot recover for any punitive damages. *Demidoff.*

Therefore, if Sidecar is liable, CDI could only recover for $5,500, or the cost of the cybersecurity investigation and the overtime for employees to assist the investigation.

Conclusion

For the reasons stated above, (1) Sidecar is likely not liable for the $25,000 transfer made prior to the end of the contract but is likely liable for the $50,000 transfer made after the end of the contract; and (2) CDI can recover only $5,500.

Question MPT-2 – July 2024 – Selected Answer 2

TO: Damien Breen
FROM: Examinee
DATE: July 30, 2024
RE: Sidecar Design Matter

MEMORANDUM

Conference Display Innovations Inc. (CDI) sent a demand letter to Sidecar Design LLC for $606,000 in damages. CDI alleges that Sidecar has violated the federal Computer Fraud and Abuse Act and Sidecar is liable for CDI's damages.

(1) The issue is whether Sidecar Design is liable to CDI under the CFAA.

Under the Computer Fraud and Abuse Act, an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" violates the Act. 18 U.S.C. § 1030(a)(2). An individual who "knowingly and with the intent to defraud" exceeds authorized access and obtains anything of value also violates the Act. *Id.* at (4).

CDI hired Sidecar to create a website and secure payment system. During this process, John Smith, a software engineer hired by Sidecar, "charged $25,000 to one of CDI's customers" and transferred those funds to his own bank account. Sidecar then finished its work and "transferred control of the website and payment system to CDI." CDI did not change its login credentials at that point and Smith charged an additional $50,000 to the same CDI customer and deposited those funds to his own bank account." The customer terminated a pending contract with CDI worth $125,000.

Smith clearly intentionally accessed a computer, with the intent to defraud, and obtain something of value. However, the issue is whether Smith's action exceeded his authorized access when he was a software engineer who was working on the project and had "full access to all the data present" in CDI's system, "including customer credit card information."

(a) Exceeding authorized access

To maintain a civil action under the CFAA, a plaintiff must show, among other things, that the defendant accessed a computer either "without authorization" or in a way that "exceeds authorized access." *HomeFresh LLC v. Amity Supply Inc.* (citing 18 U.S.C. § 1030(a)(2), 1030(a)(4)). An individual "'exceeds authorized access' only when a person accesses data that the person does not have the technical right to access." *HomeFresh,* quoting *Van Buren v. United States*. The individual must access information in areas of the computer "that are off limits to him." *Id.* In *Van Buren*, where the police officer "had a computer and login credentials that gave him access to license plate data, he did not violate the CFAA" when he used that data "in exchange for payment from a third party." *Id.* Similarly, in *HomeFresh*, where the employee "did not need to use technical means to circumvent the password protection" because he "had valid password access," he did not violate the CFAA. *Id.*

Here, Smith was a software engineer working on CDI's website and payment system, and had a password with full access to all data, including credit card information. Anyone "with the password" could "charge a customer's account with the customer's knowledge" under Sidecar's login credentials. Therefore, as an employee, Smith did not access a computer without authorization. Further, he did not exceed authorized access because he had a "technical right to access" the credit card information. *Van Buren*. Even though he used the data for a fraudulent purpose, to send the $25,000 to himself, he had the right to access the information through his employment, similar to the employees in *Van Buren* and *HomeFresh*.

(b) End of employment

Once an employee leaves a job, the employee no longer has the legal right to use the employer's computers or to use the passwords or login credentials that allow the employee access to those computers, so an employee who does so may be held liable under the CFAA. *HomeFresh*. In *HomeFresh*, where the employee left his job and continued to access customer data, he violated the Act, even though he still had password access. *Id.*

Although the first transfer of $25,000 was within the access Smith had through his employment, the second transfer may be a violation of the CFAA. Smith made the $50,000 transfer after Sidecar "finished its work and transferred control of the website and payment system to CDI." CDI did not change the passwords and Smith then made the second transfer using the same password access. Here, if the court were to find that the end of CDI's contract with Sidecar is the same as ending an employment relationship, then Smith's actions in the second transfer are a violation of the CFAA. Although he still has "password access" because CDI had not changed the password, he did not technically have access to the customer data, because Sidecar and CDI's employee-employer relationship had terminated. Although Sidecar is an independent contractor, hired only to complete the website design and payment system for CDI, they had access to CDI's information through the employment relationship, so it is likely that a court would find the continuing access to CDI's customer information a violation of the CFAA.

(2) The issue is what damages CDI can recover under the CFAA if Sidecar Design is liable.

(a) Cost of investigating and correcting the data breach

The CFAA permits recovery of losses only if the claimant's losses exceed a threshold amount of $5,000 during any one-year period. *Slalom Supply v. Bonilla* (quoting 18 U.S.C. § 1030(g)). Losses include "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." 18 U.S.C. § 1030(e)(11). A victim of hacking cannot use the violation "as a means of improving its own security or system capability." *Bonilla*. Under *Bonilla*, the employer could recover "the amount paid to its own employees to assist the cybersecurity firm during the investigation." *Id.*

Here, CDI has requested $6,000 for the cost of investigating and correcting the data breach. This amount includes $4,000 for the security firm that investigated and fixed the problem, $500 for an upgrade to its security system, and $1,500 in overtime pay to its employees for helping with the security firm's investigation. The $4,000 will likely be recoverable because the security firm's investigation includes the "damage assessment and restoring the data, program, system or information to its condition prior to the offense." However, the $500 for the upgraded security system will not be recoverable, as established by *Bonilla*, a claimant may not use the CFAA violation as a means of improving its security system. However, the $1,500 paid to CDI's employees as overtime will likely be recoverable because it is an amount "paid to [CDI's] own employees to assist the cybersecurity firm," just like in *Bonilla. Bonilla.* Therefore, of the $6,000 for the cost of investigating and correcting the breach, CDI will likely be entitled to $5,500. CDI will be eligible to file the CFAA claim based on the damages for the cost of investigating and correcting the data breach because the CFAA requires a threshold amount of only $5,000.

(b) Restitution to improperly billed customer

Compensable loss includes "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). The lost revenues and consequential damages qualify as losses only when the plaintiff experiences an interruption of service. *Bonilla*, quoting *Selvage Pharm v. George*. Where a $10 million revenue loss resulted from misappropriation of trade secrets, it was not a CFAA-qualifying loss because it "did not result from interruption in service." *Bonilla,* quoting *Next Corp. v. Adams*. However, where the interruption is only temporary, courts will still award damages, provided that the alleged damages result from the interruption. *Bonilla*, quoting *Cyranos Inc. v. Lollard*. In *Bonilla*, where the claimant experienced a four-hour shutdown of its website after a hacker "redirected two customer payments," the claimant could not recover the amount of the redirected payment because the redirection of payments occurred before the interruption. *Bonilla*. CDI shut down its website and payment system for five days, pursuant to the cybersecurity firm's advice. CDI has requested $75,000 as restitution to the improperly billed customer. This restitution does not fall under the compensable loss as defined by the CFAA. CDI can only recover lost revenues or consequential damages that it experienced as a result of an interruption of service. Although CDI had a five-day interruption of service, it has not established that the interruption resulted in any lost revenue. Although the shutdown occurred in order to investigate and correct the breach of its data, the loss did not occur during the interruption of service or as a result of the interruption of service. Therefore, because the restitution to the improperly billed customer was not a result of an interruption of service, CDI likely cannot recover the $75,000 under the CFAA.

(c) Contract with customer terminated

Lost revenue and consequential damages typically involve "such things as the deletion of critical files that cost the plaintiff a lucrative business opportunity." *Bonilla,* quoting *Ridley Mfg. v. Chan*. An award of damages specifically tied to deactivation of a website for two days during peak sales was an appropriate award of lost revenue in *Cyranos Inc. v. Lollard. Bonilla*, citing *Cyranos.*

Similarly to the restitution claim, the customer terminated a $125,000 contract with CDI before the interruption occurred. The termination of the contract was on July 9 and the website shut down did not occur until July 11. Therefore, although the actions of Smith cost CDI a lucrative business opportunity, the loss did not occur as a result of the interruption of service. The termination of the contract is more alike to the damages alleged in *Bonilla*, which were not granted, than to those in *Ridley* and *Cyranos*. Because the loss was not connected with a termination of service, CDI likely will not be able to recover the $125,000 under CFAA.

(d) Punitive damages

Damages for a violation are limited to economic damages. 18 U.S.C. § 1030(g). Courts have consistently refused to include punitive damages within the definition of economic damages and the plain language of the CFAA statute precludes an award of punitive damages. *Bonilla*; *Demidoff v. Park*.

In their demand letter, CDI alleges that Sidecar must $400,000 in punitive damages to CDI. The CFAA does not provide for punitive damages, but only for economic damages. Therefore, a court will not award CDI punitive damages under the CFAA statute and Sidecar will not be required to pay $400,000 to CDI.

Conclusion

Sidecar may be liable to CDI under the CFAA. Because Smith accessed CDI's customer information after Sidecar's work was completed and Sidecar had transferred control of the website back to CDI, Smith's transfer of $50,000 from CDI's customer to himself is likely a violation of the CFAA. Further, Sidecar may be liable for $5,500 in damages for CDI's cost of investigating and correcting data breach. However, under the CFAA, Sidecar will not be liable for the restitution to improperly billed customer, the contract with customer terminated, or the punitive damages, because they do not fall under the permitted damages under the CFAA.

Question MPT-2 – July 2024 – Selected Answer 3

MEMORANDUM

TO: Damien Breen
FROM: Examinee
DATE: July 30, 2024
RE: Sidecar Design's CFAA liability

Introduction

Our client, Sidecar Design, has been sued by its former client, CDI, because Sidecar's employee, John Smith, diverted payment from CDI's customer to himself through access credentials he received under his employment at Sidecar. You asked me to research Sidecar's potential liability under the CFAA.

(1) Is Sidecar Design Liable to CDI under the CFAA?

The CFAA provides for civil liability against a defendant who accessed a computer either "without authorization" or in a manner that "exceeds authorized access." 18 U.S.C. § 1030. The CFAA was adopted to guard against hacking. The Supreme Court has interpreted "exceeds authorized access" to include only access to data that a person does not have the "technical right" to access. *See HomeFresh* (citing *Van Buren*). Thus, the Supreme Court held, a police officer who used his valid login credentials to access a woman's license plate data on behalf of a third party in violation of a department policy restricting access to the license plate database to law enforcement purpose did not violate CFAA. *Van Buren*. The Supreme Court left open the question of whether "without authorization" also requires contravention of technical limitation on access, or may include access limitation contained in contracts or policies. The 15th Circuit has not ruled on this question, but the Franklin District Court has held that an employee violates the CFAA if he access a computer after leaving a job, even if he continues to have valid password access, because he "no longer has the legal right to use the passwords or login credentials that allow the employee access." *HomeFresh*.

Here, Smith's access to CDI's system prior to Sidecar's completion of the website likely did not violate CFAA, so Sidecar is not liable based on Smith's first deposit. As held by the Court in *Van Buren* and the court in *HomeFresh*, a person does not violate CFAA when they use valid login credentials to access a system for an impermissible purpose. Here, CDI gave Sidecar a password to CDI's payment system which gave it full access to the system, including the information used by Smith. Thus, Sidecar had valid access to the system and is liable only if Sidecare "exceed[ed] authorized access." As discussed above, exceeding authorized access does not include technically permitted access for an unauthorized purpose. Here, CDI and Sidecar had agreed that Sidecar would not use any of CDI's customer data. However, Sidecar nonetheless had valid access credentials to reach that data, so Smith's use of the information for an improper purpose does not violate CFAA because there was no "hacking" or other technical means deployed to reach the data.

Smith's access to the payment system after Sidecar completed the website, however, likely does violate CFAA. There is no binding precedent on whether someone can access information "without authorization" when there access is prohibited only be contract or policy, not by technical limitations, but the Franklin District Court has analyzed the issue. In *HomeFresh*, an employee used his login credentials and work computer to download customer information from his first employer to provider to his next employer who was a competitor of the first. In that instance, the court held that the employee's access to customer files while he was still employed by the first employer, although in violation of policy, did not violate CFAA because no technical means were required. However, the employee's actions after he left his first employer did violate CFAA because the employee lost the legal right to use the login credentials, even if they were still valid in the system and no hacking was required. *Id.*

Similarly here, while Sidecar's access to the system during the contract term did not constitute a violation, after Sidecar completed the website and its contractual relationship with CDI ended, Sidecar no longer had a "legal right" to access the system. Thus, it is likely that a court would find Sidecar liable under CFAA for Smith's access to the CDI system after the contract ended because such access was "without authorization," even if CDI had failed to change the password.

CFAA has a minimum damages requirement for a civil action of losses totaling at least $5,000 in a single year. As discussed below, this requirement is likely met so CDI's suit would be allowed under the statute.

(2) Assuming that Sidecar Design is liable, what damages, if any, can CDI recover under the CFAA?

CFAA allows a person who suffers damages or loss because of a violation to recover "compensatory damages." § 1030(g). CFAA limits damages to economic damages and restricts the definition of loss to only the costs of investigation and remedy and those incurred "because of interruption of service." *Id.* § 1030(e)-(g).

The cost of investigating and remedying the security breach are plainly within those permitted by CFAA. *Slalom.* As held by the court in *Slalom*, payment of investigatory costs to a company's own employees is recoverable as a hacking victim is not required "to rely only on external help to remedy a breach." Thus, the $4,000 paid to the security firm to investigate and the $1,500 paid to CDI's employees to assist in the investigation are recoverable as damages and bring CDI above the statutory minimum to bring suit. However, the court in *Slalom* also held that money spent to upgrade a security system does not meet the statutory requirements because the statute limits loos to costs related to restoring the system "to its condition prior to the offense." Thus, the $500 paid to the security firm to upgrade the system is not recoverable.

The court in *Slalom* and the Franklin District have interpretted the text of CFAA to limit compensable losses to only those "that result specifically from an interruption in service." Thus, the *Slalom* court rejected an employer's claim for compensation from an employee who had diverted payments to his own account. Similarly, the Franklin District Court has rejected a claim for lost revenue due to misappropriation of trade secrets. *Selvage Pharm*. Thus, a court is unlikely to award damages to CDI for the $75,000 lost due to Smith's improper billing of customers because this loss was not related to any interruption of service caused by the hacking. *See Ridley Mfg.* (involving deletion of critical files resulting in award of consequential damages); *Marx Floral* (involving alteration of system-wide passwords resulting in consequential damages). Further, the termination of the customer's pending contract with CDI is not compensable because it does not relate to any interruption in services but instead was caused by the fraudulent billing. The only compensatory damages CDI would be able to pursue are those related to the five-day website shutdown. No such damages were asserted in its demand letter.

Finally, CDI is not entitled to punitive damages under CFAA. "[T]he plain language of the CFAA statute precludes an award of punitive damages." *Demidoff.*

Thus, the maximum amount CDI will be able to recover under the CFAA claim as currently alleged is $5,500 for investigation and remedy.