Memorandum

To: Damien Breen
From: Examinee
Date: July 30, 2024
Re: Sidecar Design matter, CFAA claim

Damien,

See below for the requested memo on the Sidecar Design LLC (Sidecar) matter. Specifically, I address whether Sidecar is liable to Conference Display Innovations Inc. (CDI) under the Computer Fraud and Abuse Act (CFAA), and if so, what damages CDI may be able to recover.

Bottomline: Sidecar will be found to have *not* violated the CFAA regarding Smith's charge on June 28th for $25k, but will likely be found to have violated the CFAA regarding Smith's charge of $50k on July 5th. But CDI will not be entitled to damages for the $50k charge, nor the lost $125k contract with the customer, nor the $500 to upgrade the system, nor the $400k in punitive damages. The only damages that would be awarded for Sidecar's violation of the CFAA would be for $5.5k--the charge for the security firm and its own employees to fix the problem.

I. The CFAA in general

To maintain a civil action under the CFAA, "a plaintiff must show . . . that the defendant accessed a computer either 'without authorization' or in a way that 'exceeds authorized access." *HomeFresh LLC v. Amity Supply Inc.* (citing CFAA section 1030(a)(2), 1020(a)(4)). Here, assuming Smith's actions are imposed upon Sidecar under respondeat superior, Smith did not access CDI's computer "without authorization" because he was given a password to complete Sidecar's contract work. As a result, the sole question is whether either of Smith's actions--the charge completed on June 28th for $25k or the charge completed on July 5th for $50k--constitute him "exceed[ing] authorized access."

Under the CFAA, the term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is *not entitled* so to obtain or alter." CFAA section 1030(e)(6) (emphasis added). In *Van Buren v. United States*, the Supreme Court resolved a circuit split on the scope of "exceeds authorized access" under the CFAA. And although *Van Buren* dealth with a criminal violation of the CFAA, courts have "uniformly held that courts should apply the statute consistently in both civil and criminal contexts."

HomeFresh (citing *U.S. v. Nosal* (9th Cir.)). As a result, a court will undoubtedly find that *Van Buren* controls the civil liability claim here.

In *Van Buren*, the Court held that an individual "exceeds authorized access" *only* when a person does not have the "technical right to access" that computer. *HomeFresh* (citing *Van Buren*). This means that "an individual 'exceeds authorized access' when he access 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." *Van Buren.* The Supreme Court found that because the defendant in *Van Buren* had a computer login credential that gave him access to the customer data he then exploited for his own personal gain, he did not violate the CFAA--even though his access of that customer information violated a departmental policy of his employer.

II. Alleged violations

a. Smith's June 28th charge

Under *Van Buren*, a court could not find that Smith--and by extention Sidecar--violated the CFAA regarding Smith's charge to the customer on June 28th because he had a technical right to access the customer's account information. CDI had given Sidecar full access to its payment system, including access via passwords to customer information. Even though CDI requested that Sidecar *not* access those files, it did not create any technical barrier that prevented Smith from accessing them. Because Smith accessed the customer's information and charged them under an authorized password, he did not violate the CFAA on that date.

The Franklin District Court recently decided a case which lends further support to this conclusion. In *HomeFresh*, an employee who had computer access via passwords to customer information--though was prohibited from accessing such information under company policy--exploited that information for personal gain. Following *Van Buren*, the District Court held that because the plaintiff had "permitted [the employee] to use computers . . . that gave him access to all its data, and his login credentials gave him access to data that included customer information," the employee was "not a hacker--he did not need to use technical means to circumvent the password protection . . . because he had valid password access." *HomeFresh*. Although his access of the customer information may have violated a company policy, "it did not violate the CFAA." *Id.*

Just like in *HomeFresh*, CDI gave full access via its passwords to Smith and Sidecar--which allowed access to customer information. As a result, Smith's access of that information on June 28th--while Sidecar was still completing the project--did not require him to use technical means to access the information, and that charge is not a violation of the CFAA.

b. Smith's July 5th charge

But there is a key difference between Smith's actions on June 28th and his subsequent charge of the customer on July 5th. In the latter, Sidecar had *finished* its work and transferred control of the payment system back to CDI and its work under the contract had ended. *Then*, Smith accessed the system again to create the additional charge. The issue is whether Smith's subsequent access to CDI's system *after* his right to use the system had ended violates the CFAA. Notably, the Court in *Van Buren* "left explicitly unresolved . . . whether liability under the CFAA turns 'only on technological (or 'code-based') limitations on access or instead also looks to limits contained in contracts or policies.'" *HomeFresh* (quoting *Van Buren*).

The Franklin District Court confronted this unresolved question in *HomeFresh* and decided that if a defendant accesses a computer after "the termination of his right to use" it they may be held liable under the CFAA. *HomeFresh*. In that case, the defendant still had *technical access* to the computer because the plaintiff had not physically revoked access or changed passwords such that the defendant could not access the files. But because the defendant no longer had the "legal right to use the employer's computers or to use the passwords or login credentials that allow . . . access to those computers" he violated the CFAA. *Id.* The District Court made this holding despite the fact that "other jurisdictions have reached differing results"--such that "only technological limitations, such as password protection, will suffice to terminate access for purposes of the CFAA." *Id.*

Here, Smith's July 5th charge poses the same question. CDI--even though Sidecar instructed it to--did not change its passwords yet even though Sidecar had finished its work on the system. If a court were to follow other jurisdictions, because the passwords were not changed, Sidecar would not be liable under the CFAA for the July 5th charge. But if a court followed the Franklin District Court, and found that because Sidecar did not have the *legal* right to access the CDI system--despite still having the technical ability to do so--it could be liable for Smith's July 5th charge. Notably, given that Congress enacted the CFAA to address the "growing public concern with access to computers by hackers," and that the district court in our own jurisdiction had follow the "legal right restriction" path--a court would most likely find that Smith's charge on July 5th was a violation of the CFAA as exceeding authorized access."

III. Damages

Assuming that Sidecar violated the CFAA when Smith charged the customer account on July 5th, CDI would be entitled under the statute to "compensatory damages" if that violation resulted in "damage or loss" that exceed $5k. CFAA section 1030(g). Under the CFAA, "loss" includes "any revenue lost, cost incurred, or other consequential damages incurred *because of interruption of service*." *Id.* at section 1030(e)(11) (emphasis

added). In *Slalom Supply v. Bonilla*, the Fifteenth Circuit noted that the plain text of the CFAA limits "compensable losses *only* to those that result *specifically* from an 'interruption in service.'" *Slalom* (emphasis added). The Circuit noted that courts have given the statute a "narrow reading" and that "[l]ost revenues and consequential damages qualify as losses only when the plaintiff experiences an interruption of services.'" *Id.* (quoting *Selvage Pharm. v. George*). If a complaint does not at least allege an interruption in service, a court could even dismiss the whole complaint as the plaintiff had not suffered any damages under the CFAA. *See Selvage; Next Corp. v. Adams* (finding a $10M revenue loss from misappropriation is not a CFAA-qualifying loss). Instead, courts have found an interruption in service when a defendant had deleted critical files that cost a lucrative business opportunity, *Ridley Mfg. v. Chan*, or the defendant had altered system-wide passwords, *Marx Florals v. Teft*. A court will award losses, even if the interruption is only temporary, if "the alleged damages *result from* the interruption." *Slalom* (emphasis added).

Here, CDI has alleged an temporary interruption in service. After discovering the data breach, CDI hired the external security firm to investigate the breach, and then shut down its website for five days to fix the problem. As a result, only losses incurred by CDI that result from that interruption are recoverable under the CFAA. I will address each of the alleged damages in turn.

a. Restitution damages from improperly billed customer

Notably, because Sidecar did not violate the CFAA regarding the June 28th $25k charge, only the $50k charge on July 5th is potentially recoverable. However, even though Smith wrongly misappropriated the customer funds on July 5th, that loss to CDI was not the result of an interruption of service. Smith did not delete files or change passwords that cause an interruption of service--notably, his actions created no interruption to the system as they were not even discovered when he did them.

In *Slalom*, a defendant unquestionably violated the CFAA by hacking into the plaintiff's network and diverting customer payments--totaling $85k--to his own personal account. The plaintiff then had to investigate the breach and shut down its website for four hours. Despite the defendant's flagrant violation of the CFAA, the Fifteenth Circuit held that even though the defendant's "hacking redirected two customer payments; it did not otherwise impair or damage the functionality of [the plaintiff's] computer system." *Slalom*. Just like in *Slalom*, even though Sidecar likely violated the CFAA with the July 5th charge, Smith's actions there did not delete any files, change any passwords, or otherwise impair or damage the functionality of CDI's system. Additionally, even though an interruption *did* result due to the later investigation, Smith's actions occurred before that interruption.

Accordingly, CDI would not be able to recover any of the claimed $75k restitution loss under the CFAA.

b. Cost of investigating and correcting the breach

In *Slalom*, the Circuit held that plaintiff costs to "upgrade the security system do[] not meet the statutory requirements to "restor[e] the system." As a result, the $500 charge from the firm to CDI to upgrade the system with stronger protections are not losses that fall under the CFAA.

However, both the $4k charge to the security firm to investigate and correct the issue, as well as the cost to pay its own employees $1500 for overtime to help the investigation are likely recoverable. In *Slalom*, the Circuit held that plaintiffs "can recover the amount paid to its own employees to assist [a] cybersecurity firm during the investigation" as well as the cost to the security firm to "respond" to an offense and conduct a damage assessment. Here, the $4k charge to the firm qualify as a loss to respond to the offense and conduct an assessment. Additionally, the $1.5k cost for their own employee overtime was "related solely to working on the investigation" and is recoverable.

As a result, CDI can recover $5.5k--more than the $5k statutory minimum--for those losses related to the five day interruption in service.

c. Lost contract

As noted above, only losses resulting from an interruption in services is recoverable. Here, the $125k lost contract from the customer is not resulting from an interruption in service. The customer withdrew its contract due to the charges--not from the five day interruption in service. Notably, the customer withdrew its contract *before* the interruption in service--this is just like *Slalom*. And even though in *Ridley* a court allowed the plaintiff to recover for the loss of a lucrative business opportunity--that was because the defendant had deleted critical files of the customer's. Here, Smith did not delete any files belonging to the customer, or other cause an interruption in service that led the customer to cease the contract.

As a result, the $125k alleged damages are not recoverable.

d. Punitive Damages

Under the CFAA, only "economic damages" are recoverable. In *Slalom*, the Circuit expressly held that the CFAA does not authorize punitive damages.

As a result, the $400k punitive damage claim is not recoverable.

Conclusion

CDI is entitled to only $5.5k in damages for the violation of the CFAA by Sidecar.

Best,
Examinee

TO: Damien Breen
FROM: Examinee
DATE: July 30, 2024
RE: Sidecar Design's Liability to CDI Under the CFAA

Damien,

Please see below for my analysis of Sidecar Design's liability to Conference Display Innovations Inc ("CDI") under the Computer Fraud and Abuse Act ("CFAA"). Based on my evaluation, Sidecar is likely liable to CDI for one of John Smith's improper transfers but not the other. Additionally, based on the damages calculation under the CFAA, CDI can recover $5,500 in damages, assuming Sidecar is liable under CFAA.

Sidecar Design Is Probably Liable to CDI Under the CFAA For John Smith's Second Transfer But Is Not Liable for the First

The CFAA principally governs whether or not Sidecar will be liable to CDI based on John Smith's improper transactions via his access to CDI's payment systems. The CFAA under 18 USC §1030(a) imputes liability to anyone who intentionally accesses a computer without authorization or exceeds authorized access and whose conduct involves in fraud and the capture of anything of value. Relevant case law helps explain what it means for a party to engage in unauthorized access or exceed the scope of authorized access.

In *HomeFresh v. Amity Supply, Inc. (D. Frank. 2022),* the district court examined a matter in which an employee of HomeFresh exceeded the scope of his authorized access. HomeFresh employed a VP of HR named Flynn who was given a password-protected computer that gave him access to all of HomeFresh's files. While Flynn was told to only access personnel data, he had access to HomeFresh's customer lists, account information, and contracts. During his time at HomeFresh, Flynn downloaded information on HomeFresh's principal customers. Flynn then took a job at a rival company, Amity, but retained access to HomeFresh's confidential customer information. After he left HomeFresh, Flynn continued to download confidential customer information from HomeFresh's files until HomeFresh discovered Flynn's acces, changed his password, and removed his access from their systems.

The district court found that Flynn had not violated CFAA when he accessed HomeFresh's files during the course of his employment. In reaching this decision, the court relied on the Supreme Court decision in *Van Buren v. United States (141 S.Ct. 1648 2021).* In *Van Buren*, the defendant was convicted of a CFAA violation because he accessed a police database to

obtain a license plate number which he then sold to a third party. This was a violation of department policy but the defendant had valid access to this information. The Supreme Court overturned his conviction and found that the defendant had not exceeded authorized access. The Court specifically stated that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer that are off limits to him." Because the defendant had access to the data he obtained via his login information, he did not violate CFAA even though his behavior was a violation of department policy.

The court in *HomeFresh* applied the same logic to Flynn's initial access of HomeFresh's customer lists. It first specified that CFAA application is uniform across both civil and criminal cases, citing *U.S. v Nosal, 676 F. 3d 854 (9th Cir. 2012).* It then analyzed the civil claim against Flynn through the lens of *Van Buren*. Although Flynn was the VP of Human Resources and was only supposed to access personnel files, Flynn's login granted him full access to all of HomeFresh's files, including its customer lists. Thus, Flynn's conduct, when he accessed HomeFresh's customer files while still employed by HomeFresh was akin to the conduct of the defendant in *Van Buren*. Thus, the court held that Flynn's conduct while employed by HomeFresh was not a CFAA violation.

However, the court found that Flynn's conduct in accessing the files after departing from HomeFresh's employ could have been a violation of CFAA. The court explained the different approaches jurisdictions have taken with respect to potential CFAA violations for former employees. One approach is the code-based or technological limitations on access approach. This approach states that as long as a former employee still has valid access to the former employer's data or computer systems because the former employer has not disabled access, any access by the former employee is not a CFAA violation. The other approach is the contractual limitations approach, which holds that that when a former employee departs from his former employer, his right to access the former employer's data is terminated because the contractual relationship of employment between the parties has terminated. The court in *HomeFresh* chose to use this approach. It found that there was a dispute as to material fact about Flynn's access of HomeFresh's data after he was no longer employed by HomeFresh and went to work for Amity. It denied Amity's motion for summary judgment with respect to HomeFresh's CFAA claim with respect to Flynn downloading HomeFresh's records after he went to work for Amity.

John Smith's First Improper Transfer

Applying the law to the facts here, it is clear that Sidecar is not liable to CDI for John Smith's first improper transfer using customer payment information. CDI hired Sidecar on May 31 based on Sidecar's web design expertise to create an online payment system for CDI customers so that they can pill their CDI bills online via a credit card. In creating this payment system, CDI granted Sidecar access login information to access CDI's system. CDI repeatedly asked Sidecar not to access the customer information in the system but this fact is immaterial under CFAA. Through CDI's permission and its provision of login information to Sidecar, Sidecar had full access to all of CDI's customer data and could do things like charge a customer's account or change the deposit account to which billed funds would be sent. John Smith, in his work as a programmer for Sidecar which began on June 5, had access to all of this information. Even though he was asked not to take the information, the fact that he still had access to it validly through the login credentials CDI gave him means he did not exceed his authorized access. John Smith then used this access to charge one of CDI's customers and reroute the payment to his personal bank account. Much like the defendant in *Van Buren*, Smith had valid access to the system and his ability to reach and alter customer payment information does not constitute a CFAA violation. Sidecar did not complete the system until July 2, four days after John Smith made the first improper transfer. The first transfer Smith made, while he was working on building the system, thus does not impute liability to Sidecar under CFAA.

John Smith's Second Improper Transfer

There is a second question as to whether Smith's second transfer from CDI's customer to his own bank account after Sidecar had completed the payment system for CDI constitutes a CFAA violation for which Sidecar can be held liable. The answer to this question will turn on which approach governs for former employees who access information. As explained above, the District Court of Franklin uses the contractual limitations approach. However, this approach is not, as of yet, mandatory authority but rather is persuasive. Another District Court could feel inclined to use the code-based or technological limitations approach. If it did so, it would set up a split for the 15th Circuit to decide.

More likely however, is that the district court will follow the contractual based approach to determining if there is exceeded unauthorized access. Under this approach, once the contractual relationship has ended, an employee no longer has a right to access the systems of the other party. If he or she does so, this exceeds the scope of authorized access and constitutes a CFAA violation. Here, Sidecar completed the payment system for CDI on July 2,

2024. On July 5, 2024, three days after Sidecar completed its work, Smith again used his login credentials to access CDI's customer base, charged a customer, and rerouted payment to his account. Under the contractual limitations approach, Smith would have exceeded the scope of his authorized access in doing this. That behavior would constitute a CFAA violation. Because the Franklin District Court has expressed a willingness to use this approach, such as in *HomeFresh*, it is likely the case that Sidecar is liable for a CFAA violation based on this second transaction by John Smith.

However, if the court decides to employ a technological limits based approach, Sidecar is likely not liable. When Sidecar completed its work for CDI on July 2, it informed CDI and told CDI to change its password to its system. However, CDI failed to do so and did not change the password until July 9, four days after the second transfer. Because CDI failed to change the passwords when first advised on July 2, John Smith was able to access the system on July 5. Under the technological limits approach, Smith was not exceeding his authorized access up until the point that CDI changed its password and disabled his access to their system. Because he accessed the system on July 5 before CDI changed its password on July 9, Smith's second transfer on July 5 is not a CFAA violation under the technological limits approach.

Thus, it is likely, but not certain that Sidecar will be facing CFAA liability for John Smith's second transfer from his unauthorized access of CDI's sytems. It is certain that Sidecar will not face liability for the first transfer however, as Smith did not exceed his authorized access when he made that transfer.

Damages CDI Can Recover from Sidecar, Assuming Sidecar Is Liable, Under the CFAA Should Total $5,500

The second issue is the amount of damages CDI can recover from Sidecar assuming Sidecar is found liable for Smith's violation of CFAA. Under 18 USC §1030(a) loss is defined as any reasonable cost to the victim, any reasonable cost to the victim, including responding to the offense, conducting a damage assessment, restoring the system to its condition prior to the offense, revenue lost, cost incurred or other consequential damages *because of interruption of service*. (emphasis added). Under §1030(g), a civil action under CFAA may be maintained if the damages total at least $5,000. Damages for a violation of CFAA are limited only to economic damages.

Slalom Supply v. Bonilla (15th Cir. 2023) provides additional clarification as to which damages apply under CFAA. In *Bonilla*, a formerly discharged bookkeeper hacked into Slalom's computer system and diverted two

payments totaling $85,000 to his personal account. In response to this security breach, Slalom hired a cybersecurity firm to investigate the breach, upgraded its security system to protect against future cyberattacks, and had $1,500 of employee overtime devoted to protecting the data in its system after the hack. Slalom had to shut down its website for four hours on a Sunday morning to address the hack. Additionally, Slalom paid $85,000 out of its own pocket to the two customers affected by the breach. The District Court awarded Slalom the full amount of these damages, totaling, $92,000 Slalom also was awarded $300,000 in punitive damages by the district court.

The Court of Appeals overturned a number of these awards. First, it overturned the $1,500 cost for Slalom to upgrade its system after the breach. The court held that the CFAA does award damages for the costs related to "restoring the system to its condition prior to the offense." The statute's plain language suggests that a victim of a hacking cannot use the violation as a means of improving its own security capability. It did however uphold the costs associated with hiring the cybersecurity firm to investigate and the cost of the employee overtime to guard the company's data.

The court also overturned the $85,000 award of consequential damages. The court placed great emphasis on the fact that consequential damages must be due to an interruption of service in order for those damages to be available. Slalom paid its two disgruntled customers of its own volition. Slalom also offered no evidence of losses related to its site going offline in the morning hours. In making this finding the court cited several cases which held that consequential damages were not available due to no interruption of service. This included *Selvage Pharm v. George* in which there was a failure to allege facts constituting an interruption of service and *Next Corp v. Adams* in which a $10 million loss from a misappropriation of trade secrets was held not to be a CFAA violation because there was no interruption of service. In contrast, the deletion of critical files which cost the plaintiff a business opportunity, the alteration of system wide passwords, and a two day website outage were all found to be interruptions of service allowing for consequential damages under CFAA. *Ridely Mfg v. Chan, Marx Florals v. Teft; Cyranos Inc. v. Lollard*

Lastly, the Court of Appeals overturned the punitive damages award because economic damages are all that are allowed under CFAA and punitive damages are consistently not included in economic damages. *Demidoff v. Park*

CDI's Cost of Investigation and Remedy

Applying the case law to the damages incurred by CDI, CDI is only entitled to recover $5,500. Under the same circumstances as in *Bonilla*, CDI can recover for the cost of the cybersecurity firm it hired to investigate the outage which was $4,000. Likewise, it can recover the cost of its employee overtime necessitated by the breach, which was $1,500. However, it is not entitled to recover damages for the $500 cost it spent to upgrade its security system since *Bonilla* explicitly states that the costs of an upgrade after a hack are not contemplated by CFAA damages.

CDI's Lost Business Damages
Additionally, CDI cannot recover the $200,000 for the refund it issued to its customers or the lost contract that the disgruntled customer terminated. In order to recover those damages, CDI would need to show that the damages were caused by an interruption of service caused by John Smith's actions. However, CDI paid the customers the $75,000 refund and lost the $125,000 contract on July 9. CDI did not shut down its website and experience an interruption of service until July 11. This mirrors the conduct of Slalom Supply who refunded customers prior to any outages on its website occurring. Because these losses that CDI suffered are not directly attributable to its website being shut down, the strict language of CFAA precludes CDI from recovering the $200,000 in damages under CFAA liability imputed to Sidecar.

CDI's Punitive Damages
Lastly, CDI cannot recover $400,000 in punitive damages from Sidecar. As stated in the text of CFAA, only economic damages can be recovered in a civil claim under CFAA. As the 15th Circuit explained at the end of *Bonilla*, courts have routinely held that punitive damages are outside the scope of economic damages. The 15th Circuit reversed the award of punitive damages in that CFAA case and CDI will have no chance at obtaining punitive damages against Sidecar in this CFAA claim. The plain language of the CFA statute precludes an award of punitive damages. *Demidoff*

Thus, the total amount of damages CDI can recover from Sidecar, assuming Sidecar is liable under CFAA is limited to the cost CDI spent in hiring the cybersecurity firm and the cost of employee overtime as a consequence of John Smith's unauthorized transfer. That total amounts to $5,500.