July 2024
MPT-2
Item

CDI Inc. v. Sidecar Design

CDI Inc. v. Sidecar Design LLC

FILE

LIBRARY

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

MEMORANDUM

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

We have been consulted by Yolanda Davis, the manager of Sidecar Design LLC, an internet design firm. About a week ago, Sidecar received a letter from the attorney for a former client, Conference Display Innovations Inc. (CDI), demanding $606,000 in damages. Davis has asked for advice about what damages, if any, Sidecar Design may be required to pay to CDI.

This dispute arises from Sidecar's work on a web-based payment system for CDI. According to Davis, one of Sidecar's own employees, John Smith, accessed the payment system, billed one of CDI's customers, and transferred the money to himself.

As you'll see, CDI's demand letter identifies several different legal claims. I would like you to prepare a memorandum to me analyzing the claim that Sidecar has violated the federal Computer Fraud and Abuse Act (CFAA). Another associate is researching the remaining claims, including whether Sidecar has liability under the doctrine of *respondeat superior*. For purposes of this memorandum, however, you should assume that Sidecar is liable for Smith's actions.

Your memorandum should analyze the following two questions:

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

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

Do not include a statement of facts in your memorandum. Instead, be sure to integrate the facts as appropriate into your legal analysis.

Breen & Lennon LLP
Attorneys at Law

FILE MEMORANDUM

FROM: Damien Breen
RE: Summary of Interview with Yolanda Davis
DATE: July 26, 2024

This memorandum summarizes an interview with Yolanda Davis, the manager of Sidecar Design LLC. Sidecar is a website design and creation business. On July 23, 2024, Sidecar received a demand letter from CDI Inc., a business that designs display installations for conventions and business gatherings.

CDI contracted with Sidecar to create a website and a secure payment system so that CDI could expand its business nationwide. According to Yolanda Davis, the staff at CDI "knew nothing about websites or how to operate them." CDI and Sidecar signed a written contract; we do not yet have a copy of that contract.

Pursuant to their contract, Sidecar built a payment system that allowed CDI's customers to pay invoices from CDI with a credit card. The payment system stored credit card information for each customer. CDI used that information to bill its customers, and the system deposited the payments received into a CDI bank account. The amounts charged through this system could be substantial, from around $60,000 to over $200,000.

During the period in which it was creating the website and payment system, Sidecar had a password that gave it full access to all the data present in the system, including customer credit card information. CDI staff members knew this; indeed, CDI asked Sidecar to create the password-protected system to secure customer information. CDI also repeatedly insisted that Sidecar not use any of CDI's customer data once it had been entered, and Sidecar consistently agreed not to do so.

Nonetheless, as it built the system for CDI, Sidecar's login credentials gave it the ability to reach and even to alter customer data as well as CDI's own bank account information. This allowed anyone with the password to charge a customer's account without the customer's knowledge. For example, a person with the password could temporarily change the deposit account to which improperly billed funds would be deposited.

During this time, Sidecar hired John Smith, a software engineer, to work on the project. Smith programmed the payment system for CDI and set up the customer accounts. Unknown to anyone at Sidecar, and before the system had been completed, Smith charged $25,000 to one of CDI's customers and arranged to transfer those funds to his own bank account.

Sidecar eventually finished its work and transferred control of the website and payment system to CDI. At that point, Sidecar's work under its contract with CDI ended. CDI repeated its request that Sidecar not use any of CDI's data. In return, Sidecar advised CDI to change its login credentials for the payment system. Within two days, using the as-yet-unchanged login credentials, Smith charged an additional $50,000 to the same CDI customer and deposited those funds to his own bank account.

Shortly afterward, this CDI customer discovered the fraudulent billings and requested that CDI refund the total amount taken: $75,000. That customer also terminated a pending contract with CDI worth $125,000.

CDI immediately changed the password that Sidecar had used. CDI then hired a cybersecurity firm to investigate and remedy the data breach. That investigation identified Sidecar as the source of the data breach. Acting on the cybersecurity firm's recommendation, CDI shut its website down for five days. The security firm charged CDI $4,000 to investigate and fix the problem. The firm charged CDI an additional $500 to upgrade its security system with stronger protections. CDI estimates that it paid its own employees $1,500 in overtime to help with the security firm's investigation.

CDI's counsel sent a demand letter to Sidecar Design. The letter requested payment of damages totaling $606,000. The letter threatened several different civil causes of action against Sidecar, including one arising under the Computer Fraud and Abuse Act.

After receiving the letter, Yolanda Davis verified that CDI had changed the password to its payment system. John Smith left his position at Sidecar a few days before the first contact from CDI about the data breaches. He disappeared, and Davis is now trying to track him down, so far without success.

Breen & Lennon LLP
Attorneys at Law

FILE MEMORANDUM

FROM: Damien Breen
DATE: July 28, 2024
RE: Sidecar Design LLC

This chronology summarizes the results of my investigation into the events that occurred during and after Sidecar Design's work for CDI Inc.

5/31/2024	Sidecar Design begins work on a website and payment system for CDI.
6/5/2024	John Smith, a new Sidecar employee, begins work on the payment system. This work includes entering credit card information into customers' accounts.
6/28/2024	Using his access to CDI's payment system, Smith charges a CDI customer $25,000 and deposits that amount to his bank account.
7/2/2024	Sidecar completes building the website, and its contractual relationship with CDI ends. Sidecar instructs CDI to change the password for the payment system. CDI does not change the password.
7/5/2024	Using this password, Smith charges another $50,000 to the same CDI customer and deposits that amount to his bank account.
7/8/2024	Smith resigns from Sidecar Design and leaves no forwarding information.
7/9/2024	The customer charged by Smith contacts CDI, demanding reimbursement of $75,000. This customer also terminates a $125,000 contract with CDI.
	CDI changes the password on the payment system. CDI also pays the customer $75,000.
7/11/2024	CDI hires a cybersecurity firm to investigate and fix the data breach and assigns an employee to work with this firm. On the firm's advice, CDI shuts down its website and payment system.
7/16/2024	CDI restores its website and payment system.

Jameson & Brooks, PC
63 Lockwood Road, Suite 600
Centralia, Franklin 33758

July 19, 2024

Ms. Yolanda Davis
Sidecar Design LLC
5564 Orbit Road
Bristol, Franklin 33716

RE: Claim for Damages from CDI Inc.

Dear Ms. Davis:

This letter serves as a formal demand for payment of $606,000 to CDI Inc. as damages for losses arising from Sidecar Design's access to and use of customer data held by CDI Inc. These losses were caused by your unauthorized billing of a CDI customer and your deposit of the amounts so obtained into accounts not held by CDI.

We seek damages in the following amounts:

Cost of investigating and correcting data breach	$6,000
Restitution to improperly billed customer	$75,000
Contract with customer terminated	$125,000
Punitive damages	$400,000
TOTAL	$606,000

If you do not pay the total amount demanded in this letter within 30 days of receiving it, we will commence legal action against you. We will assert claims based on breach of contract, trespass to chattels, intentional interference with contractual relations, fraud, and violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

If you retain an attorney, we will provide further detail to that attorney about the dates and amounts of the transactions in question.

Sincerely,

Henry Brooks

Henry Brooks, Esq.
Counsel for CDI Inc.

COMPUTER FRAUD AND ABUSE ACT

18 U.S.C. § 1030: Fraud and related activity in connection with computers

(a) Whoever—

. . .

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer; [or]

. . .

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . .,

shall be punished [as provided in a separate section] . . .

(e) As used in this section—

. . .

(6) 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 accesser is not entitled so to obtain or alter;

. . .

(11) the term "loss" means 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 . . .

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves [losses to the claimant during any one-year period totaling at least $5,000]. Damages for a violation involving only [such] conduct . . . are limited to economic damages.

HomeFresh LLC v. Amity Supply Inc.
(D. Frank. 2022)

Defendant Amity Supply has moved for summary judgment seeking dismissal of all those claims by plaintiff HomeFresh LLC that are based on the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. The court grants Amity's motion in part and denies it in part.

We take the facts as stated in HomeFresh's reply to Amity's motion as true. HomeFresh employed Joseph Flynn as its Vice President of Human Resources. During his employment, HomeFresh provided Flynn with a laptop computer that allowed him password-protected access to HomeFresh's servers both in the office and remotely.

Flynn's position gave him digital access to HomeFresh's personnel policies as well as the employment records for all its employees. While his employment contract and HomeFresh's employment policies prohibited him from accessing anything but personnel data, his company-provided computers and login credentials allowed access to all HomeFresh data. Thus, as a vice president, using his login credentials, he had access to any information stored on HomeFresh's servers, of any kind, including customer lists, account information, and contracts.

HomeFresh and Amity compete as suppliers of foodstuffs to food processing companies nationwide. Amity offered Flynn a job similar to his position at HomeFresh but at a much higher salary. Flynn and Amity negotiated the terms of the new position for several weeks before finalizing it. Flynn then gave HomeFresh two weeks' notice of his resignation but did not disclose that he would be joining Amity. During those two weeks, acting at Amity's suggestion and using his HomeFresh-provided laptop and login credentials, Flynn downloaded information on HomeFresh's principal customers. After he left HomeFresh, Flynn kept the laptop; no one at HomeFresh requested that he return it or deactivated his access credentials. Flynn then used the laptop to download additional customer data.

HomeFresh did not learn of Flynn's access until one of its customers informed it that Amity had full details about the customer's contract with HomeFresh. HomeFresh hired experts to investigate and learned that the laptop assigned to Flynn had accessed HomeFresh's customer data both before and after the date that Flynn left HomeFresh's employ to join Amity. At that point, HomeFresh terminated Flynn's user account, changed the password, and sent a cease-and-desist letter to Flynn. In the letter, HomeFresh demanded

that Flynn refrain from further access to HomeFresh's data and that he return the laptop. Flynn complied with these requests.

In its complaint, HomeFresh alleges several grounds for relief from both Amity and Flynn, including violation of the CFAA. With respect to that claim, HomeFresh alleges that Flynn's access to its data was either unauthorized or beyond the scope of his authorized access. In its motion, Amity counters that Flynn's access was authorized because HomeFresh failed to create technical barriers that would prevent Flynn's access to its customer data.

Congress enacted the CFAA in 1986 to address a growing public concern with access to computers by hackers. The Act was later expanded to cover information from any computer "used in or affecting interstate or foreign commerce or communication," a provision now uniformly held to apply to any computer that connects to the internet. 18 U.S.C. § 1030(e)(2)(B); *Van Buren v. United States*, 141 S.Ct. 1648, 1652 (2021). While the CFAA initially imposed criminal penalties, Congress later amended it to permit civil actions against a violator. 18 U.S.C. § 1030(g). Courts have uniformly held that courts should apply the statute consistently in both civil and criminal contexts. *U.S. v. Nosal,* 676 F.3d 854, 858 (9th Cir. 2012).

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." 18 U.S.C. § 1030(a)(2), 1030(a)(4). In 2021, the United States Supreme Court decided *Van Buren*, which resolved a circuit split as to the meaning of the phrase "exceeds authorized access." In *Van Buren*, a police sergeant in Georgia was convicted under the CFAA after he used his work computer and login credentials to search a police database for a woman's license plate in exchange for payment from a third party. Through his work computer, the sergeant could reach the departmental database, and his login credentials gave him access to license plate information. No technical barrier to accessing that information existed. Rather, it was only a departmental policy that barred him from using that data for non-law-enforcement purposes.

The Supreme Court reversed Van Buren's conviction, concluding that an individual "exceeds authorized access" only when a person accesses data that the person does not have the technical right to access. "[A]n 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." 141 S.Ct. at 1662. Because Van Buren had a computer and login credentials that gave him access to license plate data, he did not violate the CFAA, even if the purpose for his access violated departmental policy.

In this case, HomeFresh permitted Flynn to use computers, including a laptop, that gave him access to all its data, and his login credentials gave him access to data that included customer information. Even though HomeFresh's employment policies put customer data outside the scope of Flynn's duties, he could still reach that data using HomeFresh's computers. In effect, at the time he accessed customer data, Flynn was not a hacker—he did not need to use technical means to circumvent the password protection in HomeFresh's system because he had valid password access. In short, Flynn's use of the data while still employed by HomeFresh may have violated HomeFresh's employment policies, but it did not violate the CFAA.

HomeFresh next argues that, even if Flynn's access during his employment did not violate the CFAA, any access *after* he left HomeFresh necessarily violated the CFAA because his right to use HomeFresh's computers ended when his employment ended. This argument poses a question that the Supreme Court left explicitly unresolved in *Van Buren*: 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." *Id.,* 141 S.Ct. at 1658, fn. 8.

If only technological limitations, such as password protection, will suffice to terminate access for purposes of the CFAA, then it would not be until Flynn downloaded data after HomeFresh revoked his password that his actions violated the CFAA. By contrast, if the termination of his right to use HomeFresh's computers terminated his access as defined by the CFAA, any data downloaded *after* Flynn left HomeFresh would violate the Act. Indeed, courts in other jurisdictions have reached differing results on this question. This court, however, finds the latter approach more persuasive. That is, 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. An employee who does so may be held liable under the CFAA.

For these reasons, Amity's motion for summary judgment as to any data accessed after Flynn left HomeFresh is denied. A triable issue of fact exists as to the alleged violations of the CFAA during that period. At the same time, the court grants Amity's motion as to any data Flynn downloaded while still employed by HomeFresh.

So ordered.

Slalom Supply v. Bonilla
(15th Cir. 2023)

At issue in this appeal is the district court's award of damages for violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. Plaintiff Slalom Supply (Slalom) is an online retailer of cold weather gear and sporting supplies. In 2019, Slalom hired defendant Sam Bonilla as a bookkeeper. Like many of Slalom's employees, Bonilla worked remotely from home. In October 2021, Slalom discovered that many accounts were in disarray and that Bonilla had failed to pay a key supplier. Bonilla had been devoting most of his working hours to his own consulting business.

Slalom terminated Bonilla's employment effective November 1. Bonilla's duties had covered all of Slalom's business accounts for customers, suppliers, and facilities. As a result, Bonilla had had password access to all Slalom's records using the internet from his home computer. In light of this, Slalom made sure to change all its system passwords that same day, including those passwords that had allowed Bonilla remote access.

In early December 2021, Bonilla hacked into Slalom's network and diverted two payments from customers—a total of $85,000—to his own account. After discovering this attack, and to preserve its relationship with these customers, Slalom fulfilled these orders at its own expense. Slalom then hired a cybersecurity firm to investigate the breach, which necessitated shutting down its website for four hours early on a Sunday morning during the holiday season. The investigation revealed that Bonilla had used hacking software to bypass the new passwords and had exploited his knowledge of Slalom's accounts to divert the two payments to his own account.

Two months later, Slalom sued Bonilla, asserting violations of the CFAA as well as other claims. Following a bench trial, the district court found that Bonilla had violated the CFAA and awarded Slalom damages under the Act. On appeal, Bonilla does not challenge the finding that his actions violated the CFAA but argues that the district court erred in its award of damages. We address each category of damages in turn.

Costs of Investigation and Remedy

The district court awarded Slalom $7,000 for damages associated with the cost of remedying Bonilla's hacking attack: $4,000 for the investigation, $1,500 to upgrade Slalom's

security system against future cyberattacks, and $1,500 for employee time devoted to protecting the data in its system.

To the extent that the issue of whether a defendant violated the CFAA involves the interpretation of the CFAA, it is a question of law that we review de novo. The CFAA permits recovery of "losses" only if the claimant's losses exceed a threshold amount of $5,000 during any one-year period. 18 U.S.C. § 1030(g). Bonilla argues that Slalom can recover only the cost of the investigation, that is, the $4,000 paid to the cybersecurity firm. According to Bonilla, any employee time or the amount spent to upgrade Slalom's system do not meet the CFAA's definition of compensable "losses." Under § 1030(e)(11), 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."

We agree with Bonilla that the $1,500 spent to upgrade the security system does not meet the statutory requirement that costs relate to "restoring the . . . system . . . to its condition prior to the offense." *Id*. The statute's plain language suggests that a victim of hacking cannot use the violation as a means of improving its own security or system capability. That said, Slalom can recover the amount paid to its own employees to assist the cybersecurity firm during the investigation. Nothing in the statutory language requires a hacking victim to rely only on external help to remedy a breach. Further, the district court found that the $1,500 for employee time related solely to working on the investigation and did not relate to the upgrade to Slalom's system.

Thus, we agree with the district court that Slalom had pled and proven losses sufficient to meet the statutory $5,000 requirement. We reverse only that portion of the award, $1,500, relating to the costs of upgrading the system.

Lost Business

The district court awarded Slalom $85,000 as consequential damages resulting from the breach. This amount consists of the value of the goods that Slalom shipped to customers whose payments Bonilla diverted to his own account. In support of this award, Slalom submits that the definition of compensable "loss" under the CFAA includes "any revenue lost, cost incurred, or other consequential damages incurred *because of interruption of service*." 18 U.S.C. § 1030(e)(11) (emphasis supplied). Unfortunately for

Slalom's argument, the plain text of the Act limits compensable losses to only those that result specifically from an "interruption in service."

Case law supports a narrow reading of § 1030(e)(11). "Lost revenues and consequential damages qualify as losses only when the plaintiff experiences an interruption of service." *Selvage Pharm. v. George* (D. Frank. 2018) (dismissing complaint that failed to allege facts constituting an interruption of service, e.g. installation of a virus that caused the system to be inoperable). *See also Next Corp. v. Adams* (D. Frank. 2015) ($10 million revenue loss resulting from misappropriation of trade secrets not a CFAA-qualifying loss because it did not result from interruption in service). Most cases based on lost revenue and consequential damages involve such things as the deletion of critical files that cost the plaintiff a lucrative business opportunity, *Ridley Mfg. v. Chan* (D. Frank. 2015), or the alteration of system-wide passwords, *Marx Florals v. Teft* (D. Frank. 2012). Courts have awarded such damages even where the interruption is only temporary, provided that the alleged damages result from the interruption. *Cyranos Inc. v. Lollard* (D. Frank. 2017) (affirming award of damages specifically tied to deactivation of website for two days during peak sales).

In the case at hand, Bonilla's hacking redirected two customer payments; it did not otherwise impair or damage the functionality of Slalom's computer system. The hacker did not delete any files or change any passwords in the system. The parties, however, agree that Slalom experienced a four-hour interruption in service when its website was subsequently shut down at the recommendation of experts. Slalom offered no evidence that specifically tied any losses to the four-hour shutdown of its website. To the contrary, its sales figures were comparable to those of previous years. In short, the only costs established by Slalom to have been "because of" this interruption were the amounts it paid to investigate the hack and protect its data. By contrast, Slalom's business decision to fulfill the two customers' orders happened *before that interruption*, not as a result of it. Since the interruption in service did not cause the claimed losses, we reverse the district court's award of $85,000.

Punitive Damages

Finally, the district court awarded Slalom $300,000 in punitive damages. On appeal, Bonilla argues that this award is out of proportion to the costs that Slalom incurred to remedy the breach.

We do not reach the proportionality issue because the CFAA limits the recovery of damages in civil cases to "economic damages." Courts have consistently refused to include punitive damages within the definition of "economic damages." "[T]he plain language of the CFAA statute precludes an award of punitive damages." *Demidoff v. Park* (15th Cir. 2014).

Accordingly, we affirm that portion of the judgment awarding Slalom the cost of investigating the data breach. The award of consequential and punitive damages is reversed.

So ordered.