APPENDIX

APPENDIX

TABLE OF CONTENTS

APPENDIX A

RECOMMENDED FOR PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 20a0301p.06

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

No. 19-1235

[Filed: September 09, 2020]

ROYAL TRUCK & TRAILER SALES AND SERVICE, INC., *Plaintiff-Appellant*,	)
v.	)
MIKE KRAFT; KELLY MATTHEWS, *Defendants-Appellees*.	)

Appeal from the United States District Court for the Eastern District of Michigan at Port Huron. No. 3:18-cv-10986—Robert H. Cleland, District Judge.

Argued: December 12, 2019

Decided and Filed: September 9, 2020

Before: GILMAN, KETHLEDGE, and READLER, Circuit Judges.

COUNSEL

ARGUED: Anthony M. Sciara, KOTZ SANGSER WYSOCKI P.C., Detroit, Michigan, for Appellant. Salvatore J. Vitale, VARNUM LLP, Novi, Michigan, for Appellees. **ON BRIEF:** Anthony M. Sciara, Mark F.C. Johnson, KOTZ SANGSER WYSOCKI P.C., Detroit, Michigan, for Appellant. Salvatore J. Vitale, Richard T. Hewlett, VARNUM LLP, Novi, Michigan, for Appellees.

OPINION

CHAD A. READLER, Circuit Judge. Following the abrupt resignation of two employees, Royal Truck & Trailer discovered that the employees, prior to resigning, had accessed confidential company information from their company-issued computers and cell phones and then utilized the information in violation of company policy. Royal responded by filing suit against the employees, alleging violations of the federal Computer Fraud and Abuse Act (CFAA) as well as Michigan law.

The conduct at issue might violate company policy, state law, perhaps even another federal law. But because Royal concedes that the employees were authorized to access the information in question, it has failed to satisfy the statutory requirements for stating a claim under the CFAA. Accordingly, we **AFFIRM** the district court's judgment.

BACKGROUND

Royal employed Defendants Mike Kraft and Kelly Matthews as a part of the company's sales team. In conjunction with their employment, Defendants received a copy of Royal's employee handbook. With respect to the use of company equipment, the handbook prohibited a range of conduct, including: personal activities; unauthorized use, retention, or disclosure of any of Royal's resources or property; and sending or posting trade secrets or proprietary information outside the organization. Royal also had a cell phone "GPS Tracking Policy." In accordance with that policy, "[e]mployees may not disable or interfere with the GPS (or any other) functions on a company issued cell phone," nor may employees "remove any software, functions or apps." R.8, Am. Compl., ¶ 18.

Kraft and Matthews abruptly resigned from Royal to take up employment with T-N-T Trailer Sales, one of Royal's Detroit-area competitors. Fearing that confidential company information might have been compromised, Royal launched an investigation. That hunch, the investigation later revealed, proved prescient. Shortly before his resignation, Kraft forwarded from his Royal email account to his personal one quotes for two Royal customers as well as two Royal paystubs. Kraft also contacted one of Royal's customers through Royal's email server to ask the customer to send "all the new vendor info" to Kraft's personal email account. With that, Kraft then deleted and reinstalled the operating system on his company-issued laptop, rendering all of its data unrecoverable. Eventually, Royal officials went to

Kraft's home and took possession of the laptop as well as Kraft's company-issued cell phone.

Before her resignation, Matthews did much the same. From her Royal email account, Matthews sent to Kraft's personal email account a Royal "Salesperson Summary Report" that contained confidential and proprietary sales information. She likewise forwarded an email from her Royal account to her personal one that contained customer pricing information. And as Kraft did with his company laptop, Matthews reset her company-issued cell phone to factory settings, rendering all data on the phone unrecoverable. Matthews then returned her company-issued laptop and cell phone to Royal's corporate headquarters and resigned, announcing her resignation more broadly through social media by sharing a link to a video of Johnny Paycheck's hit song, "You Can Take This Job and Shove It."

Unamused, Royal hired a "forensics expert" to conduct a "comprehensive and costly damage assessment" in an effort to restore the deleted data on the now former employees' devices. R.8, Am. Compl., ¶¶ 25–26. It later filed suit against Kraft and Matthews in federal court, alleging that their conduct violated the CFAA as well as Michigan law.

The district court, however, did not see things Royal's way. It concluded that because Kelly and Matthews were authorized to access the information obtained from their company-issued computers and cell phones, the two did not "exceed[]" their "authorized access," as those terms are used in the CFAA, by later

using the information accessed on those devices in violation of company policy. Royal filed a timely appeal.

ANALYSIS

Under our familiar standard for reviewing a district court's decision granting a motion to dismiss, we "construe the complaint in the light most favorable to the plaintiff, accept its allegations as true, and draw all reasonable inferences in favor of the plaintiff." *Jones v. City of Cincinnati*, 521 F.3d 555, 559 (6th Cir. 2008) (quoting *Directv, Inc. v. Treesh*, 487 F.3d 471, 476 (6th Cir. 2007)). Against that backdrop, we ask whether the complaint "contain[s] sufficient factual matter . . . to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

The CFAA claims. As the basis for its federal claims against Kraft and Matthews, Royal invokes § 1030(a)(2)(C) of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. That provision instructs that one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished." *Id.* § 1030 (a)(2)–(a)(2)(C). Although a violation of the CFAA can be met with criminal sanction ("shall be punished"), the Act also creates a private right of action, one that allows for civil liability where "the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." *Id.* § 1030(g); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 299 (6th Cir. 2011) (explaining that the CFAA "criminalizes certain computer-fraud crimes and

creates a civil cause of action"). Of those five subclauses, relevant here is subclause (I), which covers "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).

1. Taking all of this together, to allege a violation of § 1030(a)(2)(C), Royal must plead that: (1) Defendants intentionally accessed a computer; (2) the access was unauthorized or exceeded Defendants' authorized access; (3) through that access, Defendants thereby obtained information from a protected computer; and (4) the conduct caused loss to one or more persons during any one-year period aggregating at least $5,000 in value. At this threshold stage, Defendants do not contest the first or third elements, and we will accept, for today's purposes, that Royal's claim meets the $5,000 threshold in element four. That leaves the second element: whether Defendants' access was unauthorized, or whether Defendants exceeded their authorized access, when they sent Royal's confidential information from their work devices to their personal email accounts.

We can narrow our focus even more. Royal acknowledges that Defendants had authorization to access company information through their company email accounts, and thus does not assert that Defendants' access was without authorization. What remains for our resolution then is whether Defendants nonetheless "exceed[ed] [their] authorized access" by misusing the accessed information in violation of company policy. *Id.* § 1030(a)(2).

In answering that question, we begin with the CFAA's definitional provisions. The Act defines "exceeds authorized access" as "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). Critical to that formulation are the terms "access," "authorization," and "obtain or alter." We have previously defined the term "authorization," at least in the inverse: "[A] defendant who accesses a computer 'without authorization,'" we have said, "does so without sanction or permission." *Pulte Homes*, 648 F.3d at 304 (citing *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1132–33 (9th Cir. 2009)). "Authorization" thus means to have sanction or permission. Likewise, as to the terms "obtain" and "alter," Royal emphasizes mainly the former, which is customarily understood as "to gain" or "to attain." *Obtain*, Oxford English Dictionary Online (3d ed. 2004).

Now the term "access." It is commonly defined as some variation of "entry," generally the initial entry into something. Dictionaries include several variations of "access," one of which is "[t]he power, opportunity, permission, or right to come near or into contact with someone or something; admittance; admission." *Access*, Oxford English Dictionary Online (3d ed. 2011). Another definition describes how "access" customarily is used in a digital setting: "[t]he opportunity, means, or permission to gain entrance to or use a system, network, file, etc." A related definition describes "access" as "[t]he process or act of obtaining or retrieving data from storage." *Id.* Further reflecting how "access" is used in our technology-based society,

Oxford includes a sample use of the term, defining "[h]acking" as "the practice of gaining illegal or unauthorized *access* to other people's computers." *Id.* (emphasis in original).

Reading these definitional provisions together, it follows that in utilizing the phrase "exceeds authorized access," the CFAA targets one who initially "gain[s] entrance to . . . a system, network, or file" with "sanction or permission," and then "gain[s] or attain[s]" "information" that, in the words of the statute, she is "not entitled so to obtain . . . ." 18 U.S.C. § 1030(e)(6). Congress's use of the word "so" in the phrase "so to obtain or alter" is particularly instructive. *Id.* "So" operates here as an adverb, meaning "in the way or manner described, indicated, or suggested." *So*, Oxford English Dictionary Online (2d ed. 1989). The placement of "so" near the end of the definitional sentence refers back to the antecedent "with authorization" found earlier in the definition. That textual signal is further confirmation that one who exceeds authorized access has permission to enter a computer for specific purposes, yet later obtains (or alters) information for which access has not been authorized. Section 1030(a)(2)'s aim, in other words, is penalizing those who breach cyber barriers without permission, rather than policing those who misuse the data they are authorized to obtain.

The CFAA's "damages" and "loss" provisions further confirm the Act's narrow scope. They too appear aimed at preventing the typical consequences of hacking, rather than the misuse of corporate information in the manner alleged by Royal. "Damages" is defined with

reference to the "impairment to the integrity or availability" of data, programs, systems, or information. 18 U.S.C. § 1030(e)(8). And the definition of "loss" speaks to the costs incurred by victims in responding to an offense, assessing damages, and restoring data, programs, systems, or information, as well as the costs incurred due to interrupted service. *Id.* § 1030(e)(11). While attentive to hacking episodes and the like, this is hardly the remedial scheme one might expect in a statute intended to address the misuse of sensitive business information by an employee who uses her "authorized access" in disloyal ways. *See, e.g.*, 10 U.S.C. § 923(a)(1) (punishing members of the armed forces who access a government computer "with an unauthorized purpose" and obtain classified information).

Collectively, these interpretive clues defeat Royal's CFAA claims. The CFAA prohibits accessing data one is not authorized to access. *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012). And Royal has not contested either Kraft's or Matthews's authorization to access the company files in question. Because Defendants had authorization to access that information, their conduct did not "exceed" their "authorized access," as those terms are used in § 1030(a)(2). To be sure, Royal does allege that Kraft and Matthews later misused the information they accessed. But the CFAA does not reach that conduct.

Indeed, Congress surely knew how to say "exceeds authorized use" or otherwise proscribe using data for unauthorized purposes. *See, e.g.*, 6 U.S.C. § 482(b)(1), (b)(3) (requiring sharing of homeland security

information among federal agencies in a way that "ensure[s] that such information is not used for an unauthorized purpose"). Yet it did not do so in the CFAA. Congress's "silence" on that score "is controlling." *Lindley v. FDIC*, 733 F.3d 1043, 1055–56 (11th Cir. 2013) ("'[W]here Congress knows how to say something but chooses not to, its silence is controlling.'" (quoting *Griffith v. United States*, 206 F.3d 1389, 1394 (11th Cir. 2000))); *see also Averett v. United States Dep't of Health & Hum. Servs.*, 943 F.3d 313, 318 (6th Cir. 2019) ("Omitting a phrase from one statute that Congress has used in another statute with a similar purpose 'virtually commands the inference' that the two have different meanings." (citations omitted)).

We arrived at a similar conclusion as to the CFAA's scope in interpreting the phrase "without authorization" as used in § 1030(a)(5)(B) and (C) of the CFAA, statutory companions to § 1030(a)(2). *See Pulte Homes*, 648 F.3d 295. *Pulte Homes* involved allegations that a labor union launched a campaign of email spam and voicemails against a home builder in retaliation for firing a union employee. *Id.* at 303. We were asked to decide whether that conduct constituted accessing a "protected computer without authorization." *Id.* In holding that it did not, we noted that the defendant had permission to use phone and email communications to contact the plaintiff, emphasizing that the CFAA's authorization requirements focus narrowly on whether one's threshold access was authorized. *Id.* at 304.

Given this plain understanding of the CFAA's terms, we need not rely on the rule of lenity, as

Defendants urge. Statutory interpretation starts (and customarily ends) with the text of the statute. Out of respect for Congress's textual choices, we turn to the rule of lenity only when, unlike here, statutory language cannot otherwise be reconciled. *See United States v. Adams*, 722 F.3d 788, 804 n.8 (6th Cir. 2013) (the rule of lenity "comes into operation at the end of the process of construing what Congress has expressed, not at the beginning" (quoting *Callanan v. United States*, 364 U.S. 587, 596 (1961))). Nor is there need to resort to legislative history, an often treacherous path in its own right. *See United States v. Woods*, 571 U.S. 31, 46 n.5 (2013) ("Whether or not legislative history is ever relevant, it need not be consulted when, as here, the statutory text is unambiguous."); *Conroy v. Aniskoff*, 507 U.S. 511, 519 (1993) (Scalia, J., concurring) ("[Legislative history] is not merely a waste of research time and ink; it is a false and disruptive lesson in the law. . . . The greatest defect of legislative history is its illegitimacy."). *But see United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015) (utilizing legislative history to conclude that the CFAA was intended to address hacking, as that history consistently references "trespass" into computer systems or data as the problem the Act was meant to remedy).

2. Our interpretation today, we acknowledge, might not be the final word. The Supreme Court recently granted certiorari in *Van Buren v. United States*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 206 L. Ed. 2d 822 (Apr. 20, 2020) (No. 19-783). Although set in a criminal posture, *Van Buren* presents the Supreme

Court with the opportunity to resolve the meaning of "exceeds authorized access" as used in the CFAA.

That the Supreme Court agreed to hear *Van Buren* is likely a reflection of the lower courts' dueling interpretations of this critical passage in the CFAA. 18 U.S.C. § 1030(a)(2). As we do today, the Second, Fourth, and Ninth Circuits have also held that one who is authorized to access a computer does not exceed her authorized access by violating an employer's restrictions on the *use* of information once it is validly accessed. *See Valle*, 807 F.3d at 511–12; *WEC Carolina Energy Sols., LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *LVRC Holdings*, 581 F.3d at 1129, 1133. So too have a majority of district courts in our Circuit. *See Royal Truck & Trailer Sales & Serv., Inc. v. Kraft,* No. 18-10986, 2019 WL 1112387, at *3 (E.D. Mich. Mar. 11, 2019) (collecting cases).

That said, today's decision is in tension with those from the First, Fifth, Seventh, Eighth, and Eleventh Circuits, all of whom have more broadly interpreted "exceeds authorized access." Those courts read § 1030's statutory terms as encompassing situations where an employee has authorization to access company information but uses that information in violation of company policy. *See United States v. Rodriguez*, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (holding that an employee exceeded authorized access by obtaining company information for non-business purposes); *Int'l Airport Ctrs., LLC. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (utilizing principles of agency law to find that an employee accessed his computer "without authorization" where his authorized access was

terminated once he used the information improperly); *United States v. John*, 597 F.3d 263, 271–72 (5th Cir. 2010) (finding an employee liable for exceeding authorized access even where he had access for other purposes); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–83 (1st Cir. 2001) (holding that a former employee exceeded authorized access by violating a confidentiality agreement and accessing his former employer's website).

In addition to being less faithful to § 1030's text, this latter interpretation has the odd effect of allowing employers, rather than Congress, to define the scope of criminal liability by operation of their employee computer-use policies. Had Congress intended the seemingly sweeping result of effectively criminalizing violations of an employee handbook, it would have said so in clear terms. *See Jones v. United States*, 529 U.S. 848, 858 (2000) ("[U]nless Congress conveys its purpose clearly, it will not be deemed to have significantly changed . . . the prosecution of crimes." (internal quotation marks omitted)). Yet the CFAA does not mention such policies. Absent clear instruction, we should be hesitant to impose federal sanctions for conduct as pedestrian as checking one's private social media account on a work phone. With corporate policies sometimes written in broad and arguably vague terms, treating violations as criminal acts also risks a lack of statutory notice to employees over the precise nature of conduct now criminalized. *See*, *e.g.*, *United States v. Lopez*, 929 F.3d 783, 785 (6th Cir. 2019) (penal statutes must define the criminal offense with "sufficient definiteness that ordinary people can understand what conduct is prohibited" (quoting *Kolender v. Lawson*, 461

U.S. 352, 357 (1983))). And it risks "arbitrary and discriminatory enforcement" given the variation in those policies between companies and across industries. *Nosal*, 676 F.3d at 860; *United States v. Dunning*, 857 F.3d 342, 348 (6th Cir. 2017). All of this counsels in favor of our narrow reading of the CFAA.

Data deletion. One additional issue of federal law deserves mention. Royal also alleges that Kraft and Matthews deleted data from their work devices. And unlike the Royal customer information Kraft and Matthews were authorized to access for some purposes, Royal contends that Kraft and Matthews had no authorization to engage in data deletion.

As compared to misusing confidential information one is at least authorized to obtain, data deletion, in some circumstances, might fairly be characterized as more akin to "exceed[ing one's] authorized access." But even if Kraft and Matthews "excee[ded their] authorized access" by deleting data from their company devices, Royal's complaint does not allege that the two "thereby obtain[ed] information from [a] protected computer," a required element under § 1030(a)(2)(C). After all, as others before us have previously acknowledged, it is difficult to equate deleting data with obtaining the same. *See Experian Mktg. Sols., Inc. v. Lehman*, 2015 WL 5714541, at *7 (W.D. Mich. Sept. 29, 2015) (accessing a laptop to delete data was not obtaining information for purposes of § 1030(a)(2)(C)); *Bd. of Trustees of Pierce Twp. v. Hartman*, 2008 WL 11351291, at *4 (S.D. Ohio June 18, 2008) (deletion of data on a work device after employment had ended did not constitute "obtain[ing] information" under

§ 1030(a)(2)(C); "[r]ather, the claim is that [defendant] destroyed information without authorization"). In the context of the claim presented here, we thus reject this theory of CFAA liability as well.

State-law claims. In the absence of a viable federal claim by Royal, the district court dismissed Royal's state-law claims without prejudice. It did so in accordance with the settled rule that when a district court dismisses all claims over which it has original jurisdiction (here the CFAA claims), it may also dismiss any state-law claims before it based on supplemental jurisdiction. 28 U.S.C. § 1367(c)(3); *Gamel v. City of Cincinnati*, 625 F.3d 949, 952 (6th Cir. 2010) (noting that "[w]hen all federal claims are dismissed before trial, the balance of considerations usually will point to dismissing the state law claims, or remanding them to state court if the action was removed" (citation omitted)). We see no reason to do otherwise.

CONCLUSION

For the aforementioned reasons, we **AFFIRM** the judgment of the district court.

APPENDIX B

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

No. 18-10986

[Filed: March 11, 2019]

ROYAL TRUCK & TRAILER SALES AND SERVICE, INC.,	)
Plaintiff,	)
v.	)
MIKE KRAFT AND KELLY MATTHEWS,	)
Defendants.	)

OPINION AND ORDER GRANTING DEFENDANTS' MOTION TO DISMISS, DISMISSING WITHOUT PREJUDICE PLAINTIFF'S REMAINING STATE CLAIMS, AND DENYING AS MOOT DEFENDANTS' MOTION TO STAY DISCOVERY

Plaintiff Royal Truck & Trailer Sales and Service, Inc. ("Royal Truck") brings claim against two of its former employees, Defendants Mike Kraft and Kelly Matthews, based on Defendants' alleged

misappropriation of Plaintiff's company information prior to Defendants resigning from the company. Pending before the court are two motions filed by Defendants: a motion to dismiss (Dkt. #11) and a motion to stay discovery (Dkt. #18.) These motions have been fully briefed, and the court concludes that a hearing is not necessary. *See* E.D. Mich. 7.1(f)(2). For the reasons stated below, the court will grant Defendants' motion to dismiss, dismiss without prejudice Plaintiff's remaining state law claims, and deny as moot Defendants' motion to stay.

I. BACKGROUND

Plaintiff is a Michigan-based truck supply and service company. Both Defendants are former employees of Plaintiff who accepted employment at a competitor of Plaintiff shortly after their resignations. While working for the company, both Defendants received company laptops, cell phones, and email addresses and were permitted to access Plaintiff's customer and employee information. Defendants' access to this information, Plaintiff asserts, was limited by policies described in the Plaintiff's employee handbook. This handbook included an "Information Security/Confidentiality" policy which prohibited employees from using company information for nonbusiness purposes and sharing proprietary information with competitors. Plaintiff alleges that Defendants were familiar with these policies.

According to Plaintiff, Defendants exceeded their authorized access to their company-provided cellphones, laptops, and email accounts by accessing and using information in violation of Plaintiff's

information policies. Plaintiff specifically alleges that before resigning, Defendants forwarded customer quotes, employee paystubs, and confidential sales figures to their personal email accounts and erased information and programs from their company devices. Based on these actions, Plaintiff brings claim for violation of the Computer Fraud and Abuse Act ("CFAA") as well as state law claims for conversion, breach of the duty of loyalty, tortious inference with a business relationship, and civil conspiracy.

Defendants do not explicitly deny these allegations but rather argue that Plaintiff's allegations do not form a cognizable claim under the CFAA.[1]

II. STANDARD

Federal Rule of Civil Procedure 12(b)(6) provides for dismissal of a complaint for failure to state a claim upon which relief may be granted. Under the Rule, the court construes the complaint in the light most favorable to the plaintiff and accepts all well-pleaded factual allegations as true. *Barber v. Miller*, 809 F.3d 840, 843 (6th Cir. 2015).

Federal Rule of Civil Procedure 8 requires a plaintiff to present in her complaint "a short and plain statement of the claim showing that the pleader is

---

[1] The court notes that Defendants failed to include a statement regarding Defendants' attempt to seek concurrence as required by Local Rule 7.1(a) in either of their motions. E.D. Mich. LR 7.1(a). Plaintiff's lack of concurrence to these motions is presumed based on Plaintiff's responses. Nevertheless, the court cautions that failure to comply with the court's Local Rules can result in motions being stricken without consideration.

entitled to relief." A complaint must provide sufficient facts to "state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that defendant acted unlawfully." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* (citing *Twombly*, 550 U.S. at 555).

"A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555). "To state a valid claim, a complaint must contain either direct or inferential allegations respecting all the material elements to sustain recovery under some viable legal theory." *Boland v. Holder*, 682 F.3d 531, 534 (6th Cir. 2012) (emphasis removed) (citing *League of United Latin Am. Citizens v. Bredesen*, 500 F.3d 523, 527 (6th Cir. 2007)). Determining whether a complaint states a plausible claim for relief is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555).

III. DISCUSSION

Defendants' motion to dismiss raises a narrow issue, which currently forms a circuit split: whether the Computer Fraud and Abuse Act ("CFAA") governs situations in which employees who are authorized to

access their employer's information use that information in violation of their employer's policies. For the reasons explained below, the court finds that it does not and, therefore, the court will grant Defendants' motion to dismiss.

A. CFAA Claims

The CFAA is criminal, anti-hacking statute that also creates a private cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section[.]" 18 U.S.C. § 1030(g). The portion of the statute at issue in this case prohibits individuals from knowingly accessing a protected computer "without authorization" or in a manner that "exceeds authorized access." 18 U.S.C. § 1030(a)(2). To state a claim, Plaintiff must prove that Defendants "(1) accessed a protected computer; (2) without authorization or exceeded authorized access; and (3) there was damage or loss to plaintiff of more than $5,000 of value in a one-year period." *Senderra Rx Partners, Ltd. Liab. Co. v. Loftin*, No. 15-13761, 2016 U.S. Dist. LEXIS 173203, at *6 (E.D. Mich. Dec. 8, 2016). Defendants' motion to dismiss challenges Plaintiff's ability to satisfy the second element. Here, Plaintiff alleges that Defendants exceeded their "authorized access" in forwarding price quotes, employee pay stubs, and sales information to their personal email accounts in violation of company policies. Courts are not in universal agreement as to whether an employee's violation of company policies implicates the CFAA.

In *Ajuba Int'l, L.L.C. v. Saharia*, 871 F. Supp. 2d 671 (E.D. Mich. 2012) (Battani, J.), the court aptly summarizes the two approaches taken by courts that

have analyzed the CFAA's "exceeds authorized access" language:

> Some courts have construed the terms narrowly, holding that an employee's misuse or misappropriation of an employer's business information is not "without authorization" so long as the employer has given the employee permission to access such information. *See LVRC Holdings L.L.C. v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) (holding that that the CFAA targets the unauthorized procurement or alteration of information rather than its misuse); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F.Supp.2d 373, 385 (S.D. N.Y. 2010) ("The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation.") . . . In other words, courts adopting the narrow approach hold that, once an employee is granted "authorization" to access an employer's computer that stores confidential company data, that employee does not violate the CFAA regardless of how he subsequently uses the information.
>
> Other courts have construed the terms broadly, finding that the CFAA covers violations of an employer's computer use restrictions or a breach of the duty of loyalty under the agency doctrine. *See United States v. Rodriguez*, 628 F.3d 1258(11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*,

> 274 F.3d 577 (1st Cir. 2001). The broad approach holds that "an employee accesses a computer 'without authorization' whenever the employee, without the employer's knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty." *Guest-Tek Interactive Entm't, Inc. v. Pullen*, 665 F.Supp.2d 42, 45 (D. Mass. 2009).

Id. at 686–87.

The Sixth Circuit has not directly considered this issue. *Id*. at 686. However, two of three of courts in this district to address this issue have adopted the narrow approach. *See Senderra Rx Partners, Ltd. Liab. Co. v. Loftin*, No. 15-13761, 2016 U.S. Dist. LEXIS 173203, at *6 (E.D. Mich. Dec. 8, 2016) (Cohn, J.); *see contra Am. Furukawa, Inc. v. Hossain*, 103 F. Supp. 3d 864, 876 (E.D. Mich. 2015) (Drain, J.). Additionally, the majority of district courts in the Sixth Circuit to address this issue have adopted the narrow approach. *See Experian Mktg. Sols., Inc. v. Lehman*, No. 15-CV-476, 2015 WL 5714541, at *5 (W.D. Mich. Sept. 29, 2015) (Bell, J.); *Cranel Inc. v. Pro Image Consultants Grp., LLC*, 57 F. Supp. 3d 838, 845 (S.D. Ohio 2014) (Graham, J.); *Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc*., No. 10-CV-450, 2012 WL 2524008, *5 (W.D. Mich. June 29, 2012) (Bell, J.); *ReMedPar, Inc. v. AllParts Med., L.L.C.*, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010) (Wiseman, Jr., J.); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929 (W.D. Tenn. 2008) (Breen, J.); *Am. Family Mut. Ins. Co. v. Rickman*, 554 F.Supp.2d 766, 771 (N.D. Ohio 2008) (Zouhary, J.).

With any issue of statutory interpretation, the court begins by analyzing the plain meaning of the statute. *See Perez v. Postal Police Officers Ass'n*, 736 F.3d 736, 741 (6th Cir. 2013). The court is persuaded that the plain meaning of the CFAA necessitates the adoption of the narrow approach. As explained by the Ninth Circuit Court of Appeals in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the term "authorization" must be interpreted by its ordinary meaning because it is not defined in the statute. *Id*. at 1132. Authorization is defined as "permission or power granted by an authority." *Id*. (quoting *Authorization*, Random House Unabridged Dictionary, 139 (2001); *Authorization*, Webster's Third International Dictionary, 146 (2002)). The Ninth Circuit reasoned that this definition implies that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it." Based on this plain meaning, when an employer allows an employee to access a computer, such as in this case, an employee does not act "without authorization" even if the employee uses the computer for a personal purpose. *See id*. Therefore, the statute's "without authorization" language does not apply to situations, such as those alleged in the complaint, where the plaintiff authorized the defendant to access the information at issue.[2]

---

[2] At least some of the courts to favor the narrow approach also rely on "the rule of lenity and the statutory canon of avoiding absurd results" and "the legislative history and congressional intent" as supporting such a finding. *See, e.g.*, *Ajuba Int'l, L.L.C.*, 871 F. Supp. 2d at 687. Being mindful of "the thicket of legislative history," *United States v. Gonzales,* 520 U.S. 1, 4 (1997), the court

The court also echoes the concern raised by other courts that adopting the board approach and allowing employers to recover against employees for violating internal information polices would transform a criminal statute, initially intended to punish hackers, into a federal cause of action for a breach of the duty of loyalty. *See, e.g.*, *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008) ("The statute was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers.").

Plaintiff's CFAA claims are exclusively based on Defendants' alleged violation of company policy. (Dkt. 13, PageID 109.) The court's determination that the CFAA does not extend to such conduct, therefore, ends the court's inquiry into Plaintiff's CFAA claims.

B. State Law Claims

In the absence of any surviving claims under federal law, the court will decline to exercise supplemental jurisdiction over Plaintiff's remaining state law claims. *See Novak v. MetroHealth Med. Ctr.*, 503 F.3d 572, 583 (6th Cir. 2007) (citing 28 U.S.C. § 1367(c)(3)) ("A district court may decline to exercise supplemental jurisdiction over state law claims if it has dismissed all claims over which it had original jurisdiction."). The court will dismiss without prejudice Plaintiff's

---

merely notes these points in passing without adoption or analysis. *See id.* at 6 ("Given the straightforward statutory command, there is no reason to resort to legislative history.").

remaining claims for conversion, breach of the duty of loyalty, tortious interference, and civil conspiracy.

IV. CONCLUSION

The court is not persuaded that the CFAA applies to the misappropriation of information by employees authorized to access their company's data. Accordingly,

IT IS ORDERED that Defendants' motion to dismiss (Dkt. #11) is GRANTED. The court DECLINES to exercise supplemental jurisdiction over Plaintiff's remaining state claims and DISMISSES these claims WITHOUT PREJUDICE.

IT IS FURTHER ORDERED that Defendants' motion to stay discovery (Dkt. #18.) is DENIED AS MOOT.

s/Robert H. Cleland
ROBERT H. CLELAND
UNITED STATES DISTRICT JUDGE

Dated: March 11, 2019

I hereby certify that a copy of the foregoing document was mailed to counsel of record on this date, March 11, 2019, by electronic and/or ordinary mail.

s/Lisa Wagner
Case Manager and Deputy Clerk
(810) 292-6522