PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 24-1123

NRA GROUP, LLC

v.

NICOLE DURENLEAU; JAMIE BADACZEWSKI

NICOLE DURENLEAU

v.

NRA GROUP, LLC; STEVE KUSIC; SHELL SHARMA

JAMIE BADACZEWSKI

v.

NRA GROUP, LLC; STEVE KUSIC

NRA GROUP, LLC,

Appellant

Appeal from the United States District Court
for the Middle District of Pennsylvania
(District Court No. 1:21-cv-00715)
District Judge: Honorable Jennifer P. Wilson

Argued on January 22, 2025
Before: HARDIMAN, McKEE, and AMBRO, *Circuit Judges*

(Opinion filed: August 26, 2025)

Ivo J. Becica
OBERMAYER REBMANN MAXWELL & HIPPEL
1500 Market Street
Centre Square West, 34th Floor
Philadelphia, PA 19102

Jennifer Bruce
Paige Macdonald-Matthes **(Argued)**
OBERMAYER REBMANN MAXWELL & HIPPEL
200 Locust Street
Suite 400
Harrisburg, PA 17101

Counsel for Appellant

Cory A. Iannacone **(Argued)**
PILLAR AUGHT
4201 E Park Circle
Harrisburg, PA 17111

Counsel for Appellees

OPINION OF THE COURT

AMBRO, *Circuit Judge*

In the wrong hands, the law becomes a hammer in search of a nail. This is one such case.

While employed with the debt-collection firm National Recovery Agency (NRA), Nicole Durenleau was out sick. She urgently needed a work document, but she had no way to access it. Her friend and colleague, Jamie Badaczewski, logged in to Durenleau's computer from the office, accessed the document—a spreadsheet with Durenleau's passwords—and emailed it to Durenleau. She did so with Durenleau's express permission, but the pair's actions, including Durenleau's creation of the spreadsheet, breached workplace computer-use policies.

Separately, over several years, Durenleau altered work files in a manner that credited her for performance bonuses. Evidence shows she did so believing she was eligible for the bonuses.

All the while, the women allege, they were subject to persistent sexual harassment at NRA. (One executive even slapped Durenleau.) They filed internal complaints. Eventually, Durenleau resigned, naming the harassment as the reason, and Badaczewski was fired soon after.

Just weeks later, NRA went on the offensive. It sued the women under federal and state law for computer fraud, theft of trade secrets, civil conspiracy, breach of fiduciary duty, and common-law fraud. The women answered with federal- and

state-law counterclaims for sexual harassment, retaliation, and a hostile work environment.

On cross-motions for summary judgment, the District Court entered judgment for Durenleau and Badaczewski on all claims against them, staying their remaining sexual-harassment claims against NRA pending this appeal.

We affirm the District Court in full. In doing so, we hold for the first time that, (a) by its text and purpose, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, does not turn these workplace-policy infractions into federal crimes, and (b) passwords that protect proprietary business information are not themselves trade secrets under federal or Pennsylvania law.

I. BACKGROUND

This sprawling appeal covers several chapters in the history of a long-soured workplace. We will move through each. But as the main issue centers on the violation of some workplace computer-use policies, we start there.

Through its debt-collection operations, NRA holds volumes of personally identifiable information[1] (PII) about individual debtors. To comply with federal privacy laws, it has "developed and implemented comprehensive written data protection and computer use policies." Opening Br. 11.

These data-protection practices are layered. NRA's systems are protected by digital firewalls. Employees can

[1] "Information"—like a consumer's name, address, social security number, or email address—"that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." *Guidance on the Protection of Personally Identifiable Information*, U.S. Dep't of Labor, https://www.dol.gov/general/ppii [https://perma.cc/WGS9-7RFP] (July 18, 2025).

access the systems only when they are physically present in NRA's offices or by using a company-issued laptop and virtual private network (VPN) for remote access. (That VPN connection requires additional authentication.) Employees cannot access NRA's systems through any personal or mobile devices, but they may access their NRA email accounts on their cell phones.

A related set of strict policies sets out NRA employees' rights and responsibilities. Several are relevant here:

- Employees are forbidden from sharing credentials and passwords;
- Employees may not "attempt to receive unintended messages or access information by any unauthorized means, including imitating another system, impersonating another user, or misus[ing] legal user credentials (usernames, passwords), etc.";
- Passwords "may not be stored in readable form . . . or in any location where unauthorized person[s] might discover them";
- Employees "must maintain exclusive control of their [IDs and passwords]" and "may not share [IDs] or passwords] with others . . . for any reason";
- Employees must "take appropriate measures to protect the security and integrity of non-public customer information" and may not "allow[] unauthorized use of computer terminals or access of customer files";
- An employee may not "access or request any information [she has] no responsibility for"; and
- Employees may not "use company computer systems for personal use," and an employee "caught using a company system for anything other than logging on . . . for collections purposes . . . will be terminated immediately."

App. 2886–91 (cleaned up).

Employees acknowledge and assent to all policies at hiring; after that, they annually review those governing system credentials and passwords. These policies bound Durenleau and Badaczewski during the events in question. We recount those next.

A. While Durenleau was out sick, she and Badaczewski teamed up to solve a work problem.

Durenleau was NRA's Senior Manager of Compliance Services, and Badaczewski worked in marketing. Though apparently friends, the women did not work together or even in the same NRA office.

Durenleau had COVID in January 2021, so she was out sick for more than a week. While home, she was not given a laptop to access the NRA systems from home, nor could she come to the office. She had access only to her work email through her personal phone. Soon she would ask Badaczewski for help on a pressing matter.

1. January 6, 2021: Badaczewski logged in to the NRA systems as Durenleau at the latter's request.

Despite her illness, Durenleau was attending to work matters on the morning of January 6. She asked her supervisor, Lisa Daube, to look through papers on Durenleau's desk to see if anything needed attention. Daube found an urgent task: a letter from a Wyoming state agency, dated December 17, 2020, informing NRA that its state affiliate's license had expired and had not been timely renewed. If NRA wished to renew the license without a hearing, it needed to submit a signed copy of the letter and pay a $250 fine through the Nationwide Multistate Licensing System & Registry (NMLS) within 20 days. The deadline was *that day*.

This was concerning. Shortly after 9:00 a.m., Daube and Durenleau spoke on the phone to brainstorm a list of colleagues

with NMLS access who could pay the fine. NRA's CEO, Steve Kusic, had access. So did Durenleau. Hours passed. Kusic, now aware of the problem, made it clear he wanted it solved, and fast. He emailed Durenleau, "Please let me know how YOU are going to get this fixed by the end of business today. . . . How you do it, is your problem. . . . I am not learning NMLS today, get this License Renewed TODAY!!!" App. 19–20.

Around noon, Daube texted Durenleau to offer that either (a) NRA's IT staff team could sift through Durenleau's email to find her NMLS login or (b) Durenleau could give Daube the login information to pay it herself. Durenleau favored the latter, but she did not remember her password.

So instead, she called Badaczewski and shared her NRA system credentials. Badaczewski logged in to the NRA network as Durenleau. Next, she opened a Microsoft Excel spreadsheet created by Durenleau that contained her passwords for dozens of NRA systems and accounts.[2] Though the spreadsheet itself contained no consumer PII, many systems and accounts listed did.

Badaczewski sent Durenleau her NMLS login information from the spreadsheet. Then Durenleau texted that to Daube, who confirmed she was in the NMLS system. By the afternoon of January 6, the Wyoming licensing problem was solved.

2. January 7, 2021: Badaczewski sent Durenleau's password document to her personal and work emails.

The next afternoon, January 7, Durenleau and Badaczewski spoke by phone for about 15 minutes. During that call, Durenleau, still out sick without access to her NRA

[2] To the dismay of IT professionals everywhere, the document was titled "My Passwords.xlsx." App. 2770.

computer, again gave her login to Badaczewski, who logged in to NRA's system as Durenleau. *Id.*

This time, rather than providing Durenleau with the passwords over the phone, Badaczewski emailed the password spreadsheet to Durenleau's personal Gmail account. The email message was blank, and the subject line was simply a smiley face.[3] Eighteen minutes later, Badaczewski emailed the spreadsheet to Durenleau's NRA work email. The record suggests Badaczewski's first email to Durenleau's Gmail account was an accident—both her personal and NRA email addresses began with "ndurenleau@." App. 3275–76.

B. Durenleau altered collection records used to calculate performance bonuses.

When NRA sued Durenleau for these workplace policy violations, it also sued her for unrelated allegations of fraud stemming from her crediting herself for performance bonuses.

NRA pays bonuses to its debt collectors. Bonus-worthy performance is not defined sharply; rather, "for an NRA employee to earn a bonus, the employee would 'have to do something to the account in order to aid the consumer to make a payment.'" Opening Br. 18. According to Durenleau, this "something" might be communicating with a debtor, confirming payment, recording a debtor as deceased, and the like.

---

[3] At oral argument, counsel for NRA, describing the subject line as a "winky-face emoji," repeatedly assigned malicious intent to its use: "That password spreadsheet . . . was sent willfully and intentionally with an intent to deceive as evidenced by the winky-face emoji. . . . It's undisputed that it was a winky-face emoji." When asked whether "it's nationally known that's what a winky-face emoji means," counsel for NRA did not answer and instead changed the subject. Oral Arg. Recording 31:22–32:10.

NRA assigns debt accounts to "workgroups" to track which employees are responsible for collecting a debt and thus eligible for a bonus. From 2019 through her resignation in 2021, Durenleau, as a compliance executive, was assigned to the compliance work group. Compliance was not the primary team responsible for collections (NRA has a separate collections team), but NRA executives set up a compliance workgroup for Durenleau to track her eligibility for bonuses. There is no evidence of a clear policy governing when Durenleau—a member of the compliance team, but not a collector—was eligible to receive a collection bonus. Still, she had "permission to move select accounts [to her workgroup] based on certain circumstances." App. 3631.

In January 2021, Durenleau emailed supervisors on the collections team with a concern: collectors were moving accounts out of the compliance workgroup and into their own, thus counting those accounts toward their bonuses, when Durenleau believed they should count toward hers. Daube, Durenleau's supervisor, met her to discuss the accounts. The pair reviewed some that Durenleau believed had been moved improperly by the collections team. Daube disagreed. In her view, no one in compliance had worked on these accounts, so it was "proper for collectors to move the accounts from compliance into their [workgroups]." App. 2817.

After this conversation with Durenleau, Daube asked another NRA manager to audit all collections accounts moved into the compliance workgroup in that month of January 2021. The audit revealed Durenleau had moved 146 accounts into her workgroup, 11 of which had been moved after the debt had been collected. During the audit, Durenleau called the auditing manager and asked, "[D]id I do something wrong?" App. 742.

When the audit was complete, Durenleau admitted to moving those 146 accounts. Records show that between 2019 and her 2021 resignation, Durenleau moved some 200–300 accounts per month from the collections workgroup to the

compliance workgroup. A good number of these, worth roughly $3,000 in bonus payments, were moved *after* debt payment had been made.

In response, NRA issued Durenleau a written "Final Warning with No Suspension," disqualified her from bonus eligibility, and warned her she would be fired for any new violations. App. 3201. Durenleau acknowledged the warning in writing, and she did not dispute further whether she was eligible to receive bonuses on the accounts she had moved to her workgroup.

NRA issued that warning to Durenleau on February 2, 2021. She resigned from NRA on February 21. Badaczewski, meanwhile, was fired from NRA a month later, on March 20, the day after an internal investigation revealed that she had been the one to log in to Durenleau's account in January to access and email the spreadsheet.

C. The other half of this litigation involves allegations of sexual harassment, retaliation, and related employment claims.

Though this appeal is about NRA's claims against Durenleau and Badaczewski, their claims against NRA are intertwined, and, as we later explain, *see* Part II below, relevant to whether we have jurisdiction.

Durenleau and Badaczewski claim that, during their time at NRA, they were sexually harassed, and—when they resisted—retaliated against. On this point, we recount only some of the vast record.

Durenleau reported that soon after her 2014 hiring, the CEO, Kusic, repeatedly commented on her appearance, suggested they picture each other naked, and asked her to go skinny dipping with him. Durenleau told another NRA executive about all of this, but nothing happened. Kusic's harassment continued. Later, in one bizarre incident, he "wiped

a cheese curl over Durenleau's lips" and gave her what she called a "funny look." App. 23.

Badaczewski began working at NRA much later than Durenleau, in September 2020. She described being sexually harassed "all day, every day" during her six months of employment at NRA, counting at least 120 incidents. App. 26. Kusic told her that men liked her because she had blonde hair and large breasts, and, like with Durenleau, he often asked about her sex life and interest in various men. This continued all the way through her firing in March 2021.

For Durenleau, the end began in November 2020. One day that month, a male NRA executive found Durenleau in her office with several people who reported to her. She was on the speakerphone with a coworker, who was complaining about another NRA employee. The executive asked Durenleau's subordinates to leave, closed the door, chastised Durenleau for criticizing a coworker in front of others, then slapped her on the face.[4] That day, Durenleau reported the incident to in-house counsel. In response, counsel advised Durenleau that "a feeling of job insecurity could lead to [mis]interpreting a paternalistic pat on the cheek that felt a bit more firm than usual, followed by a quick departure. But, that interpretation appears to have been mistaken. Your job is secure." App. 25.

Durenleau went out sick with COVID not long after, in January 2021, and we have already told what happened from there: the expired NMLS license, the password spreadsheet, and Badaczewski's assistance.

Durenleau resigned in February, three months after the slap, writing in her resignation letter that she was "targeted and harassed at NRA . . . [, and t]he harassment was taken to a whole new level when [the executive slapped her]." App. 4711.

---

[4] The executive was later convicted of criminal harassment for his actions.

Durenleau explained she could not "take this [anymore]" and was "resigning to free [her]self from this environment." *Id.* The next day, her attorney sent NRA a demand letter detailing Durenleau's allegations of sexual harassment and intention to sue. Recall Badaczewski was fired the next month, when NRA discovered she was the employee who had accessed Durenleau's computer and emailed her the password spreadsheet.

D. Procedural history.

NRA filed its initial complaint in April 2021. At first, it alleged only one count: a violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, by Durenleau. It filed an amended complaint the next month, adding Badaczewski as a defendant. Against both women, NRA alleged four counts under the CFAA, claims for violating the federal Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq*.; the parallel Pennsylvania Uniform Trade Secrets Act, 12 Pa. Con. Stat. § 5301 *et seq*.; and state-law claims of civil conspiracy, breach of the common-law duty of loyalty, and—against Durenleau only—fraud.

Durenleau and Badaczewski answered in June and July 2021, respectively, raising counterclaims for sexual harassment, negligent hiring and retention, and retaliation under state and federal law. After discovery, Durenleau and Badaczewski amended their answers and counterclaims in November 2022.

The parties cross-moved for summary judgment. The District Court granted summary judgment to Durenleau and Badaczewski on all of NRA's claims against them, and it granted in part the employees' motion on the sexual-harassment and related claims, leaving some of those claims pending. NRA then moved the Court to certify its judgment for the employees under Federal Rule of Civil Procedure 54(b), which permits a district court to "direct entry of a final

judgment" for some "claims or parties" if the court "determines that there is no just reason for delay." The Court did so as to its judgment for Durenleau and Badaczewski, staying the remaining sexual-harassment and retaliation claims.

NRA timely appealed.

II. JURISDICTION AND STANDARD OF REVIEW

The District Court had jurisdiction over the federal questions presented, 28 U.S.C. § 1331, and supplemental jurisdiction over the related state-law claims, *id.* § 1367. The question of our jurisdiction is not quite as tidy.

Federal Rule of Civil Procedure Rule 54(b) allows a court to "direct entry of a final judgment" on a portion of a case's claims "only if the court expressly determines that there is no just reason for delay." But Rule 54(b) certification "is the exception, not the rule, to the usual course of proceedings in a district court." *Elliott v. Archdiocese of N.Y.*, 682 F.3d 213, 220 (3d Cir. 2012). To justify the exception, the district court must determine there has been a final disposition on a "cognizable claim" sufficient to constitute a "final judgment" and evaluate whether there is "any just reason for delay, taking into account judicial administrative interests as well as the equities involved." *Id.* (cleaned up).

Elaborating on these administrative interests and equities, we have instructed that, when assessing whether there is a "just reason for delay" under Rule 54(b), a district court consider five factors:

> (1) the relationship between the adjudicated and unadjudicated claims;
>
> (2) the possibility that the need for review might or might not be mooted by future developments in the district court;

> (3) the possibility that the reviewing court might be obliged to consider the same issue a second time;
>
> (4) the presence or absence of a claim or counterclaim which could result in set-off against the judgment sought to be made final; [and]
>
> (5) miscellaneous factors such as delay, economic and solvency considerations, shortening the time of trial, frivolity of competing claims, expense, and the like.

Berckeley Inv. Grp., Ltd. v. Colkitt, 455 F.3d 195, 203 (3d Cir. 2006).

We review a district court's Rule 54(b) certification for abuse of discretion. *Id.* at 202.

At the threshold, we note that the District Court's entry of summary judgment for Durenleau and Badaczewski on NRA's claims was a final judgment on those claims. *See* Fed. R. Civ. P. 54(b) (permitting a district court to "direct entry of a final judgment as to one or more, but fewer than all, claims").

But as we weigh the "judicial administrative interests" and "the equities," *Elliott*, 682 F.3d at 220, the first factor gives us pause. When we compare the timing of Durenleau's and Badaczewski's sexual-harassment allegations with the timing of NRA's lawsuit, the suit looks preemptive—or even retaliatory, for the employees' complaining about harassment at work. In fact, in the background section of their brief to us, Durenleau and Badaczewski describe what discovery "uncovered": a "modus operandi" among NRA executives of "responding to any complaints" of sexual harassment or mistreatment by "threatening legal action against the complainant[,] . . . which is exactly what occurred to Durenleau and Badaczewski." Answering Br. 7; *see also id.* nn.1–2 (describing such instances concerning other, former

employees who were threatened with legal action or the release of "devastating" personal and professional information after complaining about mistreatment at the hands of NRA executives).

That said, the issues here are legally distinct from those stayed at the District Court. Our consideration of NRA's claims under the CFAA, state and federal trade-secrets acts, and Pennsylvania tort law has nothing to do with sexual harassment and the women's federal- and state-law employment claims. We can resolve the merits of the claims before us independently of those stayed claims, and doing so will not offend "judicial administrative interests" or "the equities involved." *Elliott*, 682 F.3d at 220. So we conclude the District Court properly certified its ruling under Rule 54(b), giving us jurisdiction over that final judgment, 28 U.S.C. § 1291.

This matter properly before us, we review de novo the District Court's grant of summary judgment. *Canada v. Samuel Grossi & Sons, Inc.*, 49 F.4th 340, 345 (3d Cir. 2022). Our inquiry is the same as that Court's: whether, viewing the facts in the light most favorable to NRA and drawing all inferences in its favor, Durenleau and Badaczewski are entitled to judgment as a matter of law because there are no genuine disputes of material fact. *Id.*; Fed. R. Civ. P. 56(a).

III. DISCUSSION

We sift through the heap of NRA's claims against Durenleau and Badaczewski, beginning with those under the CFAA. After that, we consider whether the passwords in the spreadsheet were trade secrets, and we conclude by addressing NRA's state-law tort claims against the women.

A. The District Court correctly granted summary judgment for Durenleau and Badaczewski on NRA's CFAA claims against them.

Congress adopted the CFAA in 1986 to "stem the tide of criminal behavior" involving computers, which were becoming more commonplace in schools, offices, and homes. Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442, 1443 (2016) (quoting H.R. Rep. No. 98-894, at 4 (1984)).

Two features of the CFAA merit special mention.

First, the Act turns on the meaning of "authorization." Nearly all its provisions are triggered by someone who "accesses a computer without authorization" or by "exceeding authorized access," imposing civil and criminal liability on anyone who does so with respect to a "protected computer." *See generally* 18 U.S.C. § 1030(a). To be sure, users in today's globally integrated economy would be hard-pressed to find a computer that is *not* a "protected computer" under the statute, as the term includes any computer "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).

NRA argues that Durenleau and Badaczewski accessed and used NRA's systems in ways that were either without authorization or exceeded their authorized access. These arguments hinge on the employees' failure to heed NRA's internal computer-use policies. While courts "have long struggled to apply these concepts of accessing a computer without authorization and exceeding authorized access," Bellia, above, at 1445, we have some recent guidance. In 2021, the Supreme Court took up a case presenting what it means to use a computer in a way that "exceeds authorized access," giving us a framework to use in deciding NRA's claims. *Van Buren v. United States*, 593 U.S. 374 (2021).

Second, "a violation of any of the statute's provisions exposes the offender to both civil and criminal liability," *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 201 (4th Cir. 2012), including fines in excess of $250,000 and imprisonment for up to 20 years, 18 U.S.C. §§ 1030(c), 3571(d). Our interpretation of the statute applies uniformly in both contexts. *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). That means should we hold Durenleau and Badaczewski civilly liable for their actions, the same conduct could expose them, or others in the future who do the same, to criminal prosecution. Put bluntly: NRA asks us to make the employees' conduct a federal crime.

Thus we tread carefully, mindful of the "canon of strict construction of criminal statutes" that "ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997). This is especially important with respect to the CFAA, as "dramatic changes in technology [have] swept virtually all internet-connected devices within the statute's reach." Bellia, above, at 1444; *accord Van Buren*, 593 U.S. at 379 (the statute covers "all information from all computers that connect to the internet").

NRA argues both that the employees exceeded their authorization to access NRA's system—the computer protected under the statute—and that they did so without authorization at all. The District Court ruled the employees did neither, and we agree.

1. The employees did not exceed their authorized access to NRA's computer systems.

Van Buren compels affirming the District Court's ruling that the employees did not exceed authorized access. We explain that case before applying it to the matter before us.

a. *Van Buren* and "exceeds authorized access."

The CFAA defines "exceeds authorized access" as "access[ing] 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).

In *Van Buren*, the Supreme Court took up whether under this definition the petitioner, a former police sergeant, exceeded his authorized access to a law-enforcement computer database. 593 U.S. at 378. The department's policy allowed him to use the database's information only for legitimate law enforcement purposes, but Van Buren took a bribe, through a sting operation, to search the database for information about a woman that his briber wished to track down. *Id.* at 378–80. He was charged with a felony violation of the CFAA "on the ground that running the [woman's] license plate" for that crude purpose meant he accessed the department's database in a way that "exceed[ed] authorized access." *Id.* at 380.

The Supreme Court ruled he did not, reasoning that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information *located in particular areas of the computer*—such as files, folders, or databases—*that are off limits to him*." *Id.* at 396 (emphasis added). Van Buren's conduct did not meet this standard because he had authorization to use the police database and retrieve license-plate information. Though he obtained that information for an "improper purpose," he had authorization to do so, and his obtaining the information did not exceed that authorization. *Id.*

The Court adopted this interpretation based on "a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system," as some areas are fully "off limits."

Id. at 390, 396.[5] The majority reasoned that this "gates-up-or-down approach aligns with the computer-context understanding of *access* as *entry*." *Id.* at 390 (emphasis added). Indeed, Congress enacted the statute as increased computing and connectivity made "society more vulnerable to hacking incidents"—that is, incidents of *entry* without *access*. Bellia, above, at 1467.

Even more, the *Van Buren* Court cautioned that a mere violation of a workplace computer-use policy should not create a claim under the CFAA, as doing so "would attach criminal penalties to a breathtaking amount of commonplace computer activity." 593 U.S. at 393. Were the "exceeds authorized access" language of the CFAA to apply to "every violation of a computer-use policy, then millions of otherwise law-abiding citizens [would be] criminals." *Id.* at 394. In an example highly relevant here, the Court observed that "[e]mployers commonly state that computers and electronic devices can be used only for business purposes," so were workplace policy violations cognizable under the CFAA, "an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA." *Id.*

b. Applying *Van Buren*, we conclude Durenleau and Badaczewski did not exceed their authorized access.

The District Court faithfully applied *Van Buren* to NRA's claims that the employees' actions, which violated NRA's policies, exceeded their authorized use: Durenleau when she created the password spreadsheet, accessed her computer through Badaczewski while home on COVID leave,

[5] In doing so, the Court reserved the question of "whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." *Van Buren*, 593 U.S. at 390 n.8. We consider those latter limits here.

and asked Badaczewski to email the spreadsheet to her; Badaczewski when she logged in with Durenleau's credentials and emailed the spreadsheet. Under *Van Buren*, the "gates" of access were "up" for both women—neither hacked into NRA's systems. No doubt Durenleau and Badaczewski violated NRA's policies, but as employees they had access to the systems: Durenleau by the fact of her employment, and Badaczewski with Durenleau's credentials. No one hacked anything by deploying code to enter a part of NRA's systems to which they had no access.[6]

The District Court observed that "authorization under the CFAA has not yet been defined by the Third Circuit," App. 34 (quotation marks omitted), relying instead on a first-rate opinion by our district-court colleague, Judge Savage, that explains "an employee is 'authorized to access a computer when his employer approves or sanctions his admission to that computer," *Teva Pharms. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 670 (E.D. Pa. 2018) (quotation omitted); *accord*

[6] In the scholarship, this sensible idea that the CFAA targets hacking comes from the "code-based" approach to cybercrime. That is, a user must circumvent the operation of the computer system's code—in a word, hack—to access the computer. Durenleau and Badaczewski did not do that; in fact, they used NRA's computers within the parameters of their access. The code-based approach distinguishes hacking from what NRA alleges here, "policy-based" violations. Along with the Bellia article cited throughout, we find helpful Samantha Hourican, Note, *CFAA and* Van Buren*: A Half-Measure for A Whole-Ly Ineffective Statute*, 47 Seton Hall J. Legis. & Pub. Pol'y 30 (2023); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 Mich. L. Rev. 819 (2009); and Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003).

Miller, 687 F.3d at 204 ("[A]n employee is authorized to access a computer when his employer approves or sanctions his admission to that computer."); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) ("[A]n employer gives an employee "authorization" to access a company computer when the employer gives the employee permission to use it.").

We adopt this definition today, as it is in harmony with *Van Buren* and the definitions adopted by our sister circuits. NRA no doubt authorized Durenleau and Badaczewski to access NRA's computers when they were hired.

NRA resists this conclusion by doubling down on its arguments that the employees' violation of the workplace policies means they exceeded their access. Even more, NRA contends that because Durenleau could not access her computer from home (because of firewalls, VPNs, and other code-based protections of NRA's system), she necessarily *was* hacking by inducing Badaczewski to access Durenleau's work computer. This, NRA tells us, is distinct from *Van Buren*.

No, it is not. Durenleau could access NRA's systems and her work computer, just as Van Buren could the police database. *Company policy* prohibited her from doing so at home—just like policy prohibited Van Buren's misuse of the database—so, no question, she and Badaczewski contravened NRA's computer policies. But they had access to the system. Durenleau's access allowed her to log in to her computer, create spreadsheets (even those with her passwords), and email herself documents. She instead asked Badaczewski to do this for her; Badaczewski also was an NRA employee with authorized access to NRA's systems. Once more, in the terms

of *Van Buren*, the gates were up, even if the road signs—the NRA policies—all told the women to stop and turn around.[7]

We add that the policy implications of NRA's arguments are "breathtaking." *Van Buren*, 593 U.S. at 393. Durenleau was at home and needed a password to complete an urgent work assignment—one that, in the words of her CEO, she needed to complete "TODAY!!!" App. 20. She couldn't retrieve the password, so she asked a colleague, Badaczewski, to log in to NRA's systems with her credentials and email a helpful document. NRA asks us to make this a federal crime. We refuse. Instead, we affirm the District Court's rejection of NRA's claims that the employees "exceed[ed] authorized access." 18 U.S.C. § 1030(a)(2).

[7] Even were we to assume that Badaczewski was unauthorized to access the system using Durenleau's password, on these facts Badaczewski did not "*intentionally* . . . exceed[] [her] authorized access" under the CFAA. 18 U.S.C. § 1030(a)(2) (emphasis added). Under that assumption, still mindful of the "canon of strict construction of criminal statutes" that "ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered," *Lanier*, 520 U.S. at 266, we would conclude that "intentionally" modifies the entire phrase "exceeds authorized access." 18 U.S.C. § 1030(a)(2); *see also Rehaif v. United States*, 588 U.S. 225, 231 (2019) ("We have interpreted statutes to include a scienter requirement even where the statutory text is silent on the question. And we have interpreted statutes to include a scienter requirement even where the most grammatical reading of the statute does not support one." (cleaned up)). This interpretation is also consistent with the dangers posed by hacking—as opposed to the workplace-policy violations we see here—that the CFAA is meant to address.

2. The employees were authorized to access NRA's systems.

We turn to a closely related issue: whether Durenleau and Badaczewski, who accessed the NRA systems in violation of company policy, did so without authorization at all. Our conclusion follows logically, and easily, from the analysis above. If the employees did not *exceed* their authorization, they necessarily *had* authorization.

Still, as with the "exceeds authorization" question, NRA offers arguments premised on the employees' violations of workplace policies. As NRA puts it, the firewalls, VPNs, and so forth blocked Durenleau from accessing the NRA system while she was home, thus she had no authorization to do so; Badaczewski was not authorized to access Durenleau's files; and Durenleau, without authorization, could not give Badaczewski what she did not have. We remain unpersuaded.

Instead, we hold that, absent evidence of code-based hacking, the CFAA does not countenance claims premised on a breach of workplace computer-use policies by current employees. Because "[e]mployer-employee and company-consumer relationships are traditionally governed by [state-level] tort and contract law, . . . [s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read." *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc). Like our sister circuits, we are "unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who . . . disregard a use policy." *Miller*, 687 F.3d at 207. It bears repeating: Not only would "such an approach permit[] a system owner" to use private use policies to "dictate the contours" of a statute Congress wrote; it would "federalize[] a range of disputes that have traditionally been within the purview of state law." Bellia, above, at 1475.

Though NRA would have us "criminalize[] contract law," Kerr, n.6 above, at 1600, CFAA case law cannot bear that heavy consequence. Every case NRA cites for support contemplates circumstances wholly distinct from those here. *See United States v. Shahulhameed*, 629 F. App'x 685, 688 (6th Cir. 2015) (holding that independent contractor who was fired and instructed to "not report to work" nor "have contact with anyone" at client firm accessed computer system "without authorization" when he subsequently logged on); *Brekka*, 581 F.3d at 1136 (observing without deciding that, at summary judgment, parties did not dispute that former employee "would have accessed a protected computer 'without authorization'" had he logged in "after he left" employer); *Teva*, 291 F. Supp. 3d at 671 (describing how non-employees, "akin to hackers," induced employee to share protected information from employer's computer system). NRA does not point to, nor can we find, support in case law for its radical position.

Indeed, there are many other causes of action—breach of contract, business torts, fraud, negligence, and so on—that provide a remedy for employers when employees grossly transgress computer-use policies.[8] The CFAA is the wrong tool for NRA's project.

With today's holding, we mean to turn future litigants to other causes of action so that we do not make "millions of otherwise law-abiding citizens [into] criminals." *Van Buren*, 593 U.S. at 394. Accordingly, we affirm the District Court's grant of summary judgment for Durenleau and Badaczewski on all of NRA's claims under the CFAA.[9]

---

[8] NRA brought those claims, but as we will explain, they fail, too. *See* Part III.C, below.

[9] The District Court also ruled that NRA did not show Durenleau and Badaczewski had an "intent to defraud," a required element of a CFAA claim. App. 40–42. We need not

B. Because Durenleau's passwords did not have "independent economic value," they were not trade secrets under federal or state law.

For Durenleau's creation of the password spreadsheet and Badaczewski's emailing it to Durenleau's personal account, NRA also sued the employees for violating the federal Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1836 *et seq*., and the largely parallel Pennsylvania Uniform Trade Secrets Act (PUTSA), 12 Pa. Cons. Stat. § 5301 *et seq*.

The DTSA and PUTSA protect the same type of information, so we analyze them together. Any daylight between the two statutes is irrelevant to the claims here. *Compare Teva*, 291 F. Supp. 3d at 675 (setting out DTSA elements), *with Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102, 109 (3d Cir. 2010) (analyzing elements of PUTSA claim). Each statute protects information that (a) the owner has taken reasonable measures to keep secret, (b) "derives independent economic value, actual or potential," from being kept secret, (c) is not "readily ascertainable" by "proper means," and, (d) were it disclosed or used, would have economic value to those who cannot readily access it. 18 U.S.C. § 1839(3); 12 Pa. Cons. Stat. § 5302.

Our inquiry hinges on (b), independent economic value. "[A] compilation of data that has independent economic value can be protected as a trade secret," *Synthes, Inc. v. Emerge Med., Inc.*, 25 F. Supp. 3d 617, 706 (E.D. Pa. 2014) (quotation omitted), including a "compilation of customer data" if it "was generated in such a fashion that it constitutes intellectual property of the owner," *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 409 (E.D. Pa. 2009).

---

address that, as NRA trips on the threshold requirement of showing that the pair exceeded or acted without authorization.

As we described, Durenleau's spreadsheet contained passwords for dozens of NRA systems and third-party accounts. Many databases accessible through those accounts contained consumer PII and other private information. NRA argues those passwords were trade secrets under both the DTSA and PUTSA, so Durenleau and Badaczewski misappropriated trade secrets by creating and emailing the spreadsheet.[10] We agree with the District Court that those passwords were not trade secrets.

The password spreadsheet Durenleau created and Badaczewski emailed was certainly a "compilation of data," but it was not a "compilation of customer data" or some other "intellectual property of the owner." *Id*. Case law on this point is thin and undeveloped, but in most of those cases, the password information was bundled with other, more colorable trade secrets like raw customer information, pricing schemes, strategy documents, and so on. *See, e.g.*, *CLI Interactive, LLC v. Diamond Phil's, LLC*, No. 2:22-cv-01602-JXN-CLW, 2023 WL 1818381, at *2–3 (D.N.J. Feb. 8, 2023) (discussing alleged misappropriation of system administrator passwords, branding information, marketing concepts, photos, video, and "proprietary optimization techniques and data"); *TMX Funding, Inc. v. Impero Techs., Inc.*, No. C 10-00202 JF (PVT), 2010 WL 2509979, at *3–4 (N.D. Cal. June 17, 2010)

[10] NRA also makes a fleeting argument that the passwords, by identifying clients, constituted a "list of customers." Opening Br. 45. We find that difficult to square with its concession that it "used *pseudonyms* to identify certain customers and third[]parties listed." Opening Br. 44 n.6 (emphasis added). In any event, NRA cites no authority for the bald proposition that a customer list is a trade secret. We are persuaded that, to be considered intellectual property, such a list must also reveal the kind and quantity of customer information worthy of trade-secret protection. *E.g.*, *Spring Steels, Inc. v. Molloy*, 162 A.2d 370, 372 (Pa. 1960). Durenleau's spreadsheet did not.

(concluding allegations of "nine broad categories of trade secret information," only one of which concerned "[l]ogin and password information," were "sufficient" at Rule 12(b) stage). *But see PhoneDog v. Kravitz*, No. C 11-03474 MEJ, 2011 WL 5415612, at *5 (N.D. Cal. Nov. 8, 2011) (ruling media company's allegation of Twitter password as a trade secret was enough to survive 12(b) motion, as the account and private Twitter messages revealed customer information and business strategies, but noting necessity of "fully developed evidentiary record" for more careful consideration "on summary judgment").

Here, for its conclusion that the passwords in the spreadsheet were not trade secrets, the District Court mostly relied on a district court case that interpreted Virginia's trade-secrets law, *State Analysis, Inc. v. American Financial Services Association*, 621 F. Supp. 2d 309 (E.D. Va. 2009). We think this reliance is justified, as we accept the *State Analysis* Court's trenchant explanation that a password is "simply a series of random numbers and letters that is a barrier to" other proprietary material. *Id.* at 321. Although passwords may "have economic value" if "integral to accessing [proprietary information], they have no *independent* economic value in the way a formula or a customer list might have." *Id.* (emphasis in original). Thus, when "a plaintiff has not alleged that its passwords are the product of any special formula or algorithm that it developed, the passwords are not trade secrets." *Id.*

Before us, NRA does not allege that the passwords were the "product of any special formula or algorithm." *Id.* Rather, it misses the point entirely by arguing about the sensitivity and economic value of customer information, which the passwords were not. Those passwords granted access to client databases and other business-use information. But imagine they instead protected a website with pictures of cute puppies or a beloved couple's wedding registry. (And NRA is assuredly not in the business of chihuahuas or china sets.) Because the revealed

content would have no economic value to NRA, there is no serious claim the passwords would either. That is because it is what the passwords protect, not the passwords, that is valuable.

In any event, while the leak of actual trade secrets with independent economic value can endanger a business, NRA immediately remedied the problem by simply changing the passwords. (Query whether Coca-Cola could remedy the leak of its recipe, a quintessential trade secret, merely by changing the ingredients in Coke.) The passwords in the spreadsheet shared by Durenleau and Badaczewski were "numbers and letters," *State Analysis*, 621 F. Supp. 2d at 321, that blocked the proprietary information that did have independent economic value: NRA's business records and customer databases.

In response, NRA seeks support from our nonprecedential opinion in *Estate of Accurso v. Infra-Red Services, Inc.*, 805 F. App'x 95 (3d Cir. 2020). But in that case we did not have reason to scrutinize whether passwords can be trade secrets. A jury found Accurso had "misappropriated" a roofing company's "trade secrets," including that company's "password and ID to . . . a database containing information about pricing of certain roofing jobs, past customers, and prospective customers." *Id.* at 106. On appeal, Accurso challenged the jury's finding that the database ID and password constituted a trade secret, arguing "that Defendants did not 'own' the ID and password information." *Id.* Because Accurso's argument focused on ownership, we did not address whether the passwords had independent economic value. Rather, we assumed, without deciding, that the password information was a trade secret, concluding "[t]he jury could . . . have determined that Accurso misappropriated this information because" his using it was a "violation" of "confidence." *Id.* (quotation omitted). *Accurso* does not work the magic NRA wishes it did.

We agree with the District Court and hold that these passwords, which had no independent economic value, were not trade secrets under the DTSA and PUTSA.

C. All three of NRA's state-law tort claims fail.

Based on the employees' actions to access Durenleau's computer and email the spreadsheet, NRA sued Durenleau and Badaczewski for civil conspiracy and breach of the common-law duty of loyalty. It also sued Durenleau for fraud for her altering of performance-bonus records. We affirm the District Court's judgment for Durenleau and Badaczewski on each of these state-law counts.

1. NRA's claim of civil conspiracy fails because there is no object of the conspiracy and the employees did not act maliciously.

NRA alleges civil conspiracy on the ground that Durenleau and Badaczewski conspired to violate various federal and state statutes. Because there was no such violation, and because NRA cannot show the employees acted with the required malicious intent, NRA loses.

"Claims for civil conspiracy under Pennsylvania common law," as NRA's claim here, "must be based upon an independent underlying civil cause of action." *Bro-Tech*, 651 F. Supp. 2d at 418. Along with proving that civil violation, the plaintiff must show it was the object of a conspiracy. *Gen. Refractories Co. v. Fireman's Fund Ins.*, 337 F.3d 297, 313 (3d Cir. 2003). A plaintiff must also show "[p]roof of malice"—that the conspiracy was committed with "intent to do an unlawful act or to do an otherwise lawful act by unlawful means" and "an intent to injure . . . absent justification." *Thompson Coal Co. v. Pike Coal Co.*, 412 A.2d 466, 472 (Pa. 1979). This is a demanding standard: malicious intent must be the "*sole* purpose" of the conspiracy. *Bro-Tech*, 651 F. Supp. 2d at 419 (emphasis in original) (quotation omitted). Put another way, "proof of acts which are equally consistent with

innocence" is "not sufficient" to prove malice. *Scully v. US WATS, Inc.*, 238 F.3d 497, 516 (3d Cir. 2001) (quoting *Fife v. Great Atl. & Pac. Tea Co.*, 52 A.2d 24, 27 (Pa. 1947)).

For two reasons, NRA cannot succeed on its claim of civil conspiracy.

First, there is no viable free-standing cause of action, *Bro-Tech.*, 651 F. Supp. 2d at 418, so even had Durenleau and Badaczewski conspired, there is no object of that conspiracy. NRA pled violations of the CFAA, DTSA, and PUTSA as the causes of action underlying its civil-conspiracy claim. As we have explained, *see* Parts III.A and III.B above, Durenleau and Badaczewski did not violate those statutes, so NRA's conspiracy claim fails at the threshold.

Second, and for good measure, NRA cannot show malice. Its best argument is an invitation to speculate wildly: the employees "communicated via text and cell phone numerous times" on the days when Badaczewski accessed Durenleau's files. Opening Br. 48. NRA asks us to rule in its favor because the employees have not "provided any legitimate business reason for their actions." Opening Br. 49. This is wrong twice. For starters, the employees have repeatedly said that they communicated to help Durenleau solve the looming licensing registration problem. *See, e.g.*, App. 3274 (Badaczewski's deposition, in which she states Durenleau "had no way of accessing her files" while "on COVID leave" and "she called me to . . . send over something so she could do her job"); App. 3163–64 (Durenleau's deposition, in which she explains she "needed" the "Excel file to get passwords"). But even if the employees hadn't explained this, it is NRA's *own* burden, as the plaintiff, to prove malice. The best it can muster is "proof of acts which are equally consistent with innocence," evidence that is "not sufficient." *Scully*, 238 F.3d at 516 (quotation omitted).

2. Durenleau and Badaczewski did not breach their common-law duty of loyalty because they did not compete with NRA.

NRA alleges that Durenleau's creation of the password spreadsheet and Badaczewski's assistance in emailing it combine to show the employees violated their duty of loyalty, which required them to act in NRA's best interest.[11] At best, this argument overreads Pennsylvania law on an employee's duty of loyalty; at worst, it would create civil liability for a wide array of employee infractions. We reject it.

Pennsylvania law "dictates that an employee, as the agent of [her] employer, owes [that] employer a duty of loyalty." *Synthes*, 25 F. Supp. 3d at 667. Nested in the broader duty of loyalty are specific obligations: to avoid competing with the employer, aiding the employer's competitors, or using the property or confidential information of the employer "for the [employee's] own purpose[s] or those of a third party." *Id.* (citing Restatement (Third) of Agency §§ 8.04, 8.05 (2006) and *Reading Radio, Inc. v. Fink*, 833 A.2d 199, 211 (Pa. Super. Ct. 2003)).

So to prove a duty-of-loyalty breach, NRA must show (1) that Durenleau and Badaczewski intentionally or negligently failed to act in good faith and solely for NRA's benefit in their employment, (2) that NRA was injured, and (3) that their failure to act solely for NRA's benefit was a "real factor" in causing NRA's injuries. *McDermott v. Party City*

[11] In its summary-judgment briefing at the District Court, NRA argued Durenleau's failure to renew timely the Wyoming license was yet another breach of this duty. The District Court ruled NRA forfeited this argument by not including it in its initial or amended complaints. NRA does not challenge that ruling here.

Corp., 11 F. Supp. 2d 612, 626 n.18 (E.D. Pa. 1998) (citing Pa. Suggested Standard Civil Jury Instructions § 4.16 (1991)).

Even if we spot NRA the last two elements, it cannot prove that the employees' actions satisfy the first, which requires showing Durenleau and Badaczewski did not act for NRA's benefit. Given all we know about the events in question, we agree with the District Court that there is "no evidence that Durenleau or Badaczewski used the information in any way other than to resolve the licensing issue." App. 48.

Still, NRA resists this ruling by arguing that, actually, "[e]vidence of competition is *not* required to support a claim" for breach of the duty of loyalty, Opening Br. 49 (emphasis added), characterizing some cases as holding that the duty also requires an employee to "conduct the employer's business in the employer's best interest, attentively and responsibly." Opening Br. 50–51. Left unexamined, this principle might support a claim that Durenleau's maintenance of the password spreadsheet, in violation of NRA's security policies, was not "attentive[]" or "responsibl[e]." *Id.* But each of the cases NRA cites for this invented duty still involves competition in some flavor; none finds a breach simply because an employee violated workplace policies. *Solid Wood Cabinet Co. v. Partners Home Supply*, 2015 WL 1208182, at *7–8 (E.D. Pa. Mar. 13, 2015) (finding employee may have diverted some of his former employer's business to a competitor, his later employer); *PNC Mortg. v. Superior Mortg. Corp.*, 2012 WL 628000, at *26 (E.D. Pa. Feb. 27, 2012) (reasoning former bank employees may have misappropriated customer lists, documents, and other confidential information when hired by competitor); *Westfield Grp. v. Campisi*, 2006 WL 328415, at *19 (W.D. Pa. Feb. 10, 2006) (in *fully* inapplicable circumstances, finding possible breach where lender did not inform borrowers of unfavorable loan terms, which lender should have known borrowers could not afford). Nothing in these cases looks as benign as what we have here.

At its core, the duty of loyalty owed by an employee under Pennsylvania law presumes that "no [wo]man can serve two masters." *Onorato v. Wissahickon Park, Inc.*, 244 A.2d 22, 25 (Pa. 1968) (citing Matthew 6:24). An employee has a duty not to compete, to look out for the employer's financial and competitive interests, and not to arrogate the employer's assets or business opportunities for herself. NRA cannot prove Durenleau and Badaczewski breached their duties, so we affirm.

3. Durenleau did not commit fraud by collecting bonuses on accounts she believed entitled her to bonus payments, even if that belief was mistaken.

NRA claims Durenleau committed fraud by moving accounts into the compliance workgroup, entitling her to bonus payments that NRA does not believe she earned. To succeed on its claim of fraud under Pennsylvania law, NRA must prove Durenleau moved the accounts to her workgroup knowing those transfers were false or with other intent to deceive NRA. *SodexoMAGIC, LLC v. Drexel Univ.*, 24 F.4th 183, 205 (3d Cir. 2022). The District Court ruled she did not possess the required knowledge that she was deceiving or defrauding NRA. We agree.

NRA has not shown a genuine dispute, Fed. R. Civ. P. 56(a), as to Durenleau's mental state. As evidence of her fraudulent intent, NRA offers that Durenleau, during the audit of the accounts she moved, asked an executive, "[D]id I do something wrong?"; could not point to a written policy allowing her to move the accounts; and did not challenge the written warning she received after the audit. App. 742. (She resigned soon after, instead.) To counter NRA's allegations, Durenleau has introduced evidence that different rules applied to her as head of compliance and that she thought she was following them.

At bottom, while there may be a dispute about whether there was a different policy for Durenleau's bonus payments and what that policy required, NRA has not shown a genuine dispute about the legally relevant question: whether Durenleau committed fraud by moving the accounts with knowledge she was making a false representation or with intent to deceive NRA. *SodexoMAGIC*, 24 F.4th at 205. As the District Court reasoned, NRA's evidence at best requires we speculate that Durenleau's (1) confusion about the policy, (2) asking whether she did something wrong, and (3) silence despite discipline all combine to show an intent to deceive. But "[s]peculation and conjecture may not defeat a motion for summary judgment." *Wharton v. Danberg*, 854 F.3d 234, 244 (3d Cir. 2017) (quotation omitted). Because NRA offers nothing more, we affirm.

* * *

The CFAA does not reach these violations of workplace computer-use policies, the passwords were not trade secrets, and each of NRA's state-law tort claims flunks a critical element. For these reasons, we affirm the District Court's judgment for Durenleau and Badaczewski on all of NRA's claims against them.