No. _____

United States Court of Appeals for the Third Circuit

NRA GROUP, LLC,

Applicant,

v.

NICOLE DURENLEAU AND JAMIE BADACZEWSKI,

Respondents.

APPLICATION FOR RECALL AND STAY OF THE MANDATE PENDING THE FILING AND DISPOSITION OF A PETITION FOR WRIT OF CERTIORARI

OBERMAYER REBMANN
MAXWELL & HIPPEL LLP

Paige Macdonald-Matthes
Ivo J. Becica (*Admission Pending*)
Jennifer Bruce (*Admission Pending*)
200 Locust Street, Suite 400
Harrisburg, PA 17101
(t) 717-234-9730
PMM@obermayer.com
Ivo.becica@obermayer.com
Jennifer.bruce@obermayer.com

Counsel for Applicant

PARTIES TO THE PROCEEDING AND RELATED PROCEEDINGS

This application arises from a precedential opinion and mandate issued by the United States Court of Appeals for the Third Circuit.

Applicant is NRA Group, LLC, a Pennsylvania limited liability company.

Respondents are Nicole Durenleau and Jamie Badaczewski, citizens of Pennsylvania.

The proceedings below were:

1. *NRA Group LLC v. Durenleau*, *et al.,* No. 1:21-CV-00715 (M.D. Pa. Dec. 19, 2023).
2. *NRA Group, LLC v. Durenleau*, *et al.*, No. 24-1123 (3d Cir. Aug. 26, 2025), panel reh'g granted and opinion vacated, 153 F.4th 1333 (3d Cir. Oct. 7, 2025), and amended and superseded on reh'g, 154 F.4th 153 (3d Cir. 2025), *en banc* rehearing denied and opinion aff'd, No. 24-1123 (3d Cir. Nov. 11, 2025).

CORPORATE DISCLOSURE STATEMENT

Per Supreme Court Rule 29, Applicant NRA Group states that it has no parent companies or publicly-held companies with a 10% or greater ownership interest.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page No(s)**

Statutes

Rules

To the Honorable Samuel Alito, Associate Justice of the Supreme Court of the United States and Circuit Justice for the Third Circuit:

Applicant, NRA Group, LLC ("NRA" or "Applicant"), by and through its counsel, *Obermayer Rebmann Maxwell & Hippel,* respectfully applies for a recall and stay of the mandate issued by the United States Court of Appeals for the Third Circuit pending the filing and disposition of a forthcoming petition for writ of certiorari ("Petition") pursuant to 28 U.S.C. § 2101(f) and Rule 23.

INTRODUCTION

This case raises unanswered questions left in the wake of this Court's decision in *Van Buren v. United States*, 593 U.S. 374 (2021), regarding the extent of employer protections under the Computer Fraud and Abuse Act ("CFAA"). Simply put, in this case two of NRA's now former employees circumvented NRA's computer use policies and code-based access restrictions to access NRA's computer system and send a highly confidential "Password Spreadsheet" to one of the employees' personal Gmail accounts while she was off-duty and on a leave of absence. A panel of the Third Circuit categorically rejected any potential application of the CFAA to these circumstances and affirmed the District Court's grant of summary judgment dismissing NRA's CFAA claims, despite the plain language of the CFAA which compels a different result. Accordingly, as to the CFAA, NRA's forthcoming petition for writ of certiorari will present the following questions:

1. In *Van Buren v. United States*, 593 U.S. 374 (2021), the Court articulated a "gates up/gates down" formulation for determining whether an

employee exceeded his authorized access to an employer computer system under the Computer Fraud and Abuse Act ("CFAA") but expressly reserved the question of whether employer contracts and policies could support a finding of no authorization. The question now presented is whether, in its recent precedential decision, the Third Circuit impermissibly narrowed the CFAA in contravention of the plain language of the statutory text by holding that, absent evidence of code-based hacking, the CFAA definitively forecloses all employer claims premised on a breach of workplace computer-use policies by current employees.

2. Whether the Third Circuit inappropriately inserted a heightened scienter requirement into its analysis in contravention of the plain language of the CFAA and this Court' s holding in *Van Buren*, specifically with regard to the Court's analysis of Respondent Badaczewski's conduct in accessing a computer in excess of her authorization by using Respondent Durenleau's password.

OPINIONS BELOW

The Third Circuit's precedential opinion is reported at 153 F.4th 1333 (3d Cir. 2025), and it is reproduced at App. 1a - 37a. The District Court's Order and Opinion entering summary judgment is not reported but is available at *NRA Group, LLC v. Durenleau*, *et al*., No. 24-1123, 2023 WL 8789992 (3d Cir. Aug. 26, 2025), and is reproduced at App. 38a -103a.

JURISDICTION

The Third Circuit reissued the mandate on November 18, 2025. (3d. Cir. ECF 67). On December 10, 2025, NRA filed a Motion to Recall the Mandate with the Third

Circuit. (3d. Cir. ECF 68). The Third Circuit denied the Motion to Recall the Mandate on December 17, 2025. (3d Cir. ECF 69). This Court has jurisdiction to entertain and grant an application for a recall and stay of the mandate pending the filing of a petition for writ of certiorari under 28 U.S.C. § 2101(f); *see also* S. Ct. R. 23.3.

STATEMENT OF THE CASE

This case raises important questions about the applicability of the CFAA to employees who skirt both code and policy-based computer access and usage restrictions—a novel issue for this Court and one expressly left open by this Court's *Van Buren* decision. Here, the undisputed facts demonstrate that Respondent Nicole Durenleau enlisted another employee who she did not supervise, Respondent Jamie Badaczewski, to access an area of NRA's computer system that she was not authorized to access and email a "Password Spreadsheet", (compiled without authorization), to Durenleau's personal Gmail account, unencrypted, while Durenleau was home on a leave of absence without a device capable of accessing NRA's systems. On two separate occasions on January 6 and 7, 2021, Appellees not only knowingly violated NRA's cybersecurity policies against password sharing and remote access, but also intentionally bypassed the company's firewalls to enter areas of NRA's computer system that were off-limits to Appellees and stole valuable confidential and proprietary information.

In the wake of this extraordinary betrayal and theft, NRA expended significant sums on cybersecurity professionals to not only investigate the extent of the harm caused by Appellees' surreptitious misconduct, but also take additional security

measures to safeguard highly confidential and sensitive Personal Identifying Information (PII) that it is statutorily required to protect from being improperly, and/ or unlawfully accessed. To further compound the financial harm caused by Appellees unlawful actions, NRA also discovered that Durenleau further violated NRA's policies by manipulating NRA's debt collection accounting system to receive (albeit, improperly), bonus compensation.

NRA sued Appellees for violations of the CFAA, DTSA, the Pennsylvania Uniform Trade Secrets Act ("PUTSA"), civil conspiracy, and breach of common law duty of loyalty, as well as a claim of fraud against Durenleau. (M.D. ECF 1, 8). In response, each of the Appellees leveled allegations of sexual harassment and retaliation against NRA and its executives in the form of counterclaims that have not yet been adjudicated. (M.D. ECF 24, 25).

Despite numerous undisputed facts indicating that both employees violated NRA's written computer use policies that restricted both employee use and access to its computer network, the District Court summarily disposed all of NRA's claims on summary judgment presumably based on the Court's assessment, (albeit an improper one), of NRA's direct case being one of a proverbial "David v. Goliath" situation. In making this assessment, the District Court substituted its own discretion over the express language of NRA's contracts with its employees, resulting in an outcome that runs contrary to the CFAA and this Court's recent holding in *Van Buren*.

On January 25, 2025, NRA appealed the erroneous decision to the Third Circuit. (3d Cir. ECF 1). Oral argument was held where it was quickly apparent that

the judges of the panel, and specifically Judge Ambro, were transfixed with the sensational allegations presented by Respondents' Counterclaims, rather than the CFAA issues presented by NRA's appeal. *E.g.,* (Q: . . . My first question is, would your client have sued the employees if the employees didn't claim that they were sexually harassed. A: Of course, but the fact of the matter is that the District Court dismissed all of Appellees post-employment retaliation claims. . . ."). [1]

After oral argument was held, on August 26, 2025, Third Circuit Court of Appeals issued a precedential opinion authored by Judge Ambro affirming the Middle District's grant of summary judgment on all of NRA's claims. (3d. Cir. ECF 53). The panel relied in large part on this Court's decision in *Van Buren v. United States*, 593 U.S. 374 (2021), and erroneously found that Respondents had both accessed NRA's systems with authorization and had not exceeded their authorization. Notably, the panel improperly considered the purpose of the Respondents' unauthorized access, which is irrelevant to the "gates up/gates down" formulation set forth by this Court in *Van Buren.* As such, a proper reading of *Van Buren* does not compel affirmance in this case, but in fact supports reversal and remand to resolve multiple material disputes of fact.

Accordingly, NRA petitioned for rehearing on September 8, 2025. (3d Cir. ECF 57). On October 10, 2027, panel rehearing was granted and the August 26, 2025, opinion was vacated. (3d Cir. ECF 60). The panel filed an Amended Precedential

[1] An official recording of the oral argument is found on the Third Circuit's website at https://www2.ca3.uscourts.gov/oralargument/audio/24-1123NRAGroupLLCv.Durenleauetal.mp3 .

Opinion which included limited modifications from the panel's original opinion, and which did not cure, and in some cases exacerbated, the initial basis for rehearing. NRA thus filed a second Petition for Rehearing *En Banc* on October 20, 2025. (3d Cir. ECF 64).[2] NRA's second Petition for Rehearing *En Banc* was denied on November 10, 2025. (3d Cir. ECF 66). It was noted, however, that Judge Chung voted for rehearing. *Id.*

On December 10, 2025, NRA filed a Motion with the Third Circuit to Recall the Mandate Pending the Filing and Disposition of a Petition for Writ of Certiorari. (3d Cir. 68). The Third Circuit denied the Motion on December 17, 2025. (3d Cir. ECF 69). NRA thus requests that this Honorable Court stay the mandate pending the filing and disposition of the forthcoming Petition for Writ of Certiorari to prevent irreparable harm to NRA if it is compelled to proceed to trial on Respondents' counterclaims prior to a determination on the forthcoming Petition.

REASONS FOR A RECALL AND STAY OF THE MANDATE

To obtain a stay pending filing and disposition of a petition for writ of certiorari, an applicant must show "(1) a reasonable probability that four Justices will consider the issue sufficiently meritorious to grant certiorari; (2) a fair prospect that a majority of the Court will vote to reverse the judgment below; and (3) a likelihood that

[2] The Third Circuit erroneously issued the mandate on October 16, 2025, prior to NRA's filing of the second Petition for Rehearing despite the fact that the original opinion had been vacated and replaced by an amended opinion. Accordingly, NRA filed a Motion to vacate the mandate, which was granted on October 27, 2025.

irreparable harm will result from the denial of a stay." *Maryland v. King*, 567 U.S. 1301, 1302 (2012). Applicant meets this test.

I. There is a Reasonable Probability that this Court will Grant Certiorari and a Significant Possibility of Reversal

Supreme Court Rule 10 provides a non-exclusive list of reasons that the Supreme Court will consider in determining whether to grant a petition for writ of certiorari, including when a United States Court of Appeals has: "(a). . . issued a decision in conflict with the decision of another United States court of appeal on the same important matter . . . or has so far departed from the accepted and usual course of judicial proceedings. . .as to call for an exercise of this Court's supervisory power" and "(c) … decided an important question of federal law that has not been, but should be, settled by this Court, or has decided an important federal question in a way that conflicts with relevant decision of this Court." In its forthcoming petition for writ of certiorari, Appellant intends to rely primarily on these factors.

Indeed, the Third Circuit's Amended Precedential Opinion (3d Cir. ECF 61) entirely disregarded the plain language Computer Fraud and Abuse Act ("CFAA") and eviscerated the ability of employers to seek redress under the statute for unauthorized computer access by their employees. As a matter of first impression, the Third Circuit panel held that employees do not exceed their access by accessing systems—even if done in contravention of code-based and physical access restrictions and in express violation of company policy—as long as employees are generally permitted to access the employer's system by virtue of their employment. (3d Cir ECF 61 at 23) ("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"). The panel erroneously claimed that such result was compelled by *Van Buren*, 593 U.S. 374 (2021), yet the Supreme Court in *Van Buren* specifically left open the issue of whether authorization must turn on only technical or "code-based" limitations on access, or whether limitations contained in employer contracts or policies can also support a finding of no authorization. *See Van Buren,* 593 U.S. 374 at 390 n.8 ("For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."); *see also Vox Marketing Group v. Prodigy Promos*, 556 F. Supp. 3d 1280, 1285 (D. Utah 2021) ("It does not follow, however, that hacking a password is the *only* way that one can obtain access 'without authorization.' As explained, this proposition is not supported by *Van Buren"*). Furthermore, the panel's reliance on Respondents' supposedly innocent purpose is not only belied by the facts (construed, as they must, in Appellant's favor), but fundamentally conflicts with *Van Buren*'s "gates up/gates down" formulation for determining authorization under the CFAA, which explicitly disclaims any reliance on the user's purpose in accessing the system. NRA's pending Petition for Writ of Certiorari will highlight the conflicts between the panel's holding and *Van Buren,* as well as the decisions of the Fourth and Ninth Circuits in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (noting that if an employee "is given full access to the information, provided he logs in with his username and password" but instead uses another employee's login to copy information, he "does so in a manner he was not authorized 'to so obtain.'") and *WEC*

Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012) (citing *Nosal* and observing that "if an employee has complete access to information with his own username and password, but accesses information using another employee's username and password, he also obtains information 'in a manner' that is not authorized."). By using another employee's password to access areas of the computer that she was not authorized to access, Respondent Badaczewski absolutely engaged in the exact conduct described as unauthorized by *Nosal* and *WEC Carolina*, and her purpose in doing so is irrelevant pursuant to *Van Buren*.

The Third Circuit's Amended Precedential Decision (3d Cir. ECF 61) was plainly based on an incomplete and exaggerated policy-based analysis and a clear bias in favor of Respondents' counterclaims that were not before the court on appeal. The Opinion provides:

> 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. 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.

(3d Cir. ECF 61 at 24.)

Not only did the Amended Opinion misapprehend facts surrounding the two separate instances where the Respondents' actions violated NRA's clear policies regarding data security, but the panel also disregarded the fact that this case was brought as a private civil cause of action as permitted by the statute, 18 U.S.C.A. §

1030(g). Thus, it was entirely inappropriate for the panel to suggest that NRA's interpretation would impose federal criminal liability on Durenleau and Badaczewski. The CFAA explicitly provides for private civil actions and does not provide a carveout or a different standard for imposing liability if the perpetrators of an actionable computer fraud under the CFAA happen to be employees. Moreover, the panel's policy analysis was entirely one-sided. The panel opinion failed to consider the implications of its holding for employers seeking to secure their networks from internal hacking, particularly modern forms of hacking (such as phishing) that do not require traditional "code based" hacking methods. Although *Van Buren* explicitly declined to limit employers' ability to restrict access to their computer systems through employment policies, *Van Buren*, 593 U.S. 374 at 390 n.8, the panel categorically slammed that door shut. Clearly, the Third Circuit panel were blinded by Respondents' allegations of sexual harassment and failed to consider the serious ramifications their decision created for employers across the United States. *See, e.g.,* Amended Opinion at 11-13 (section titled, "The other half of this litigation involves allegations of sexual harassment, retaliation, and related employment claims."). In light of this decision, employers are now left with an untenable dilemma. Regardless of following best practices and implementing robust computer access policies backed by code-based restrictions, there is no legal recourse under the CFAA if an employee violates these restrictions. Of course an employee may be terminated, but the reality is that a breach, whether internal or external, results in significant costs to an employer including forensic investigations, legal fees, potential regulatory fines,

customer and employee notifications, system repairs, business disruption, reputational damages, etc. The panel's failure to consider this substantial outcome from their holding simply does not comport with the plain language and intent of the CFAA.

II. Applicant Will Suffer Irreparable Harm Absent a Recall and Stay of the Mandate

Without a recall and stay of the mandate, NRA will face severe and certain prejudice if Defendants'/Counterclaim Plaintiffs' claims more forward to trial prior to the United States Supreme Court's review, consideration, and ruling on NRA's forthcoming Petition for Writ of Certiorari. If NRA is compelled to proceed to trial on Counterclaim/Plaintiffs' remaining counterclaims, NRA will be deprived its due process rights by virtue of the jury hearing only Counterclaim Plaintiffs' claims rather than the interrelated facts supporting both NRA's direct claims, as well the overlapping facts that serve as a defense to the remaining counterclaims.

During the pendency of NRA's Third Circuit appeal, the proceedings below were stayed. (Middle District ECF 204). After the mandate was reissued by the Third Circuit, NRA filed a Motion to Recall the Mandate Pending Filing and Disposition of a Petition for Writ of Certiorari to the Third Circuit (3d Cir. ECF 68). While NRA's Motion to Recall the Mandate was pending, NRA filed a Motion for Further Stay of Proceedings with the Middle District. (M.D. ECF 214). After a telephonic status conference was held, the Middle District determined to hold its decision whether to continue the stay of proceedings in abeyance. On December 17, 2025, the Third Circuit denied the Motion to Recall the Mandate, (3d Cir. ECF 69), and accordingly

NRA requests that this Honorable Court recall the mandate. Simultaneous with the filing of this Application, NRA is notifying the Middle District of its request to this Court.

The stay sought by this Application is finite, limited in duration, and would not harm Respondents as their remaining counterclaims are preserved below. Respondents, who have both left NRA and are currently gainfully employed elsewhere, have not alleged any ongoing harm that must be prevented in this case and therefore, there is no need to rush to trial. *See Barbato v. Crown Asset Mgmt. LLC*, No. CV 3:13-2748, 2019 WL 1922083, at *2 (M.D. Pa. Apr. 30, 2019) ("the Plaintiff seeks statutory damages only under the amended complaint and has not alleged any actual and/or continuing harm . . . there is a reduced need to reach a speedy resolution where there is no alleged ongoing harm that must be prevented").

CONCLUSION

For the foregoing reasons, NRA Group LLC respectfully requests that this Court grant its application for a recall and stay of the mandate pending the filing and disposition of a petition for writ of certiorari.

Respectfully submitted,

OBERMAYER REBMANN
MAXWELL & HIPPEL LLP

Paige Macdonald-Matthes, Esquire
Paige Macdonald-Matthes (Pa. I.D. No. 66266)
Ivo J. Becica (Pa. I.D. No. 207013)
Admission Pending
Jennifer Bruce (Pa. I.D. No. 329351)
Admission Pending
200 Locust Street, Suite 400
Harrisburg, PA 17101
(t) 717-234-9730
PMM@obermayer.com

Dated: December 18, 2025

APPENDIX TABLE OF CONTENTS

APPENDIX

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: October 7, 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 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,

[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).

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.

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. Kusic, now aware of the problem but apparently not of this progress, made it clear he wanted the issue 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.

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 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

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

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.

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

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. 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

[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.

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, 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 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

[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).

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]

[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)

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. 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

---

(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. Even if Badaczewski knew she was violating company policy against password sharing, she thought she was acting permissibly because Durenleau asked her to help her complete her work. So even assuming Badaczewski exceeded her authorized access, and even assuming that violated company policy, we would hold she did not intentionally exceed her authorized access because she testified repeatedly in her deposition that she believed she was doing what her supervisors wanted her to do.

the employees "exceed[ed] authorized access." 18 U.S.C. § 1030(a)(2).

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*,

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

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]

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.

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

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).

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

[10] NRA also makes a fleeting argument that the passwords, by identifying clients, constituted a "list of customers." Opening Br. 45. However, 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.

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) (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,

[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.

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 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.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

NRA GROUP, LLC, Plaintiff, v. NICOLE DURENLEAU and JAMIE BADACZEWSKI, Defendants/Counterclaim Plaintiffs, v. NRA GROUP, LLC, STEVE KUSIC, and SHELL SHARMA Counterclaim Defendants.	:	Civil No. 1:21-CV-00715 Judge Jennifer P. Wilson

ORDER

AND NOW, on this 19th day of December, 2023, in accordance with the accompanying memorandum of law, **IT IS ORDERED AS FOLLOWS**

1. The motion for summary judgment filed by Defendants/Counterclaim Plaintiffs Nicole Durenleau and Jamie Badaczewski, Doc. 158, is **GRANTED**. The Clerk of Courts is directed to enter judgment in favor of Nicole Durenleau and Jamie Badaczewski on Plaintiff/Counterclaim Defendant NRA Group's amended complaint, Doc. 8.

2. The motion for summary judgment filed by Plaintiffs/Counterclaim Defendants NRA Group, Steve Kusic, and Shell Sharma, Doc. 161, is **GRANTED IN PART** and **DENIED IN PART**. Specifically, the motion for summary judgment is granted with respect to Durenleau's quid pro quo sexual harassment claims, the portions of Durenleau's retaliation claims that deal with conduct that occurred after she left NRA, and Jamie Badaczewski's retaliation claims. The Clerk of

Courts is directed to enter judgment in favor of NRA Group, Steve Kusic, and Shella Sharma on Counts II and V of Durenleau's counterclaims, Doc. 142, and Counts III and VI of Badaczewski's counterclaims, Doc. 143. The motion for summary judgment is denied with respect to Durenleau's hostile work environment claims and retaliation claim regarding conduct while she was employed at NRA and the constructive discharge claim, Counts I, III, IV, VI, Doc. 142. The motion for summary judgment is denied with respect to Badaczewski's hostile work environment claim, Counts I, Doc. 143.

3. A status conference is scheduled for January 9, 2024 at 11:30 a.m. to discuss the status of this case. The parties shall call-in to the conference calling number 877-336-1828, using the access code 2529544.

s/Jennifer P. Wilson
JENNIFER P. WILSON
United States District Judge
Middle District of Pennsylvania

Dated: December 19, 2023

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

NRA GROUP, LLC, Plaintiff, v. NICOLE DURENLEAU and JAMIE BADACZEWSKI, Defendants/Counterclaim Plaintiffs, v. NRA GROUP, LLC, STEVE KUSIC, and SHELL SHARMA Counterclaim Defendants.	:	Civil No. 1:21-CV-00715 Judge Jennifer P. Wilson

MEMORANDUM

Before the court is a motion for partial summary judgment filed by NRA Group ("NRA") (Plaintiff and counterclaim Defendant), Steve Kusic ("Kusic") and Shell Sharma ("Sharma") (counterclaim Defendants), and a motion for summary judgment filed by Nicole Durenleau ("Durenleau") and Jamie Badaczewski ("Badaczewski") (Defendants and counterclaim Plaintiffs). (Docs. 158, 161.) In its amended complaint, NRA alleged that Defendants Durenleau and Badaczewski committed violations of the Computer Fraud and Abuse Act ("CFAA"), both the federal and state trade secrets act, breach of common law duty of loyalty, civil conspiracy, and fraud. (Doc. 8.) In their amended answers, Durenleau and

Badaczewski allege they were subjected to various forms of sex-based harassment under Title VII and the Pennsylvania Human Relations Act ("PHRA"). (Docs. 142, 143.) In its motion for summary judgment, NRA argues that there are no genuine issues of material fact, and it is entitled to judgment as a matter of law on both the claims it raises in the amended complaint and the counterclaims against it. In their motion for summary judgment, Durenleau and Badaczewski argue there are no genuine issues of material fact, and they are entitled to judgment as a matter of law on NRA's claims against them. For the reasons that follow, the court will grant Durenleau and Badaczewski's motion for summary judgment, and grant in part and deny in part NRA, Kusic, and Sharma's motion for summary judgment.

FACTUAL BACKGROUND AND PROCEDURAL HISTORY[1]

NRA is an "accounts receivable management company." (Doc. 174, ¶ 1.) Kusic is, and was at all relevant times, the Chief Executive Officer of NRA. (Doc. 162-8, ¶ 1.) Sharma is, and was at all relevant times, the Chief Operating Officer of NRA. (Doc. 174, ¶ 411.) Durenleau started working at NRA on September 15, 2014, as a collector. (*Id.* ¶¶ 430–31.) During her time at NRA, Durenleau was

[1] In considering the cross-motions for summary judgment, the court relied on Doc. 174 which includes NRA's statement of material facts (Doc. 161-5) along with Durenleau's and Badaczewski's responses to these facts. The combined nature of this document made it easier for the court to determine whether and to what extent facts were disputed. In accordance with the relevant standard for deciding a motion for summary judgment, the court relied on the uncontested facts, or where the facts were disputed, viewed the facts and deduced all reasonable inferences therefrom in the light most favorable to the nonmoving party. *See Doe v. C.A.R.S. Prot. Plus, Inc.*, 527 F.3d 358, 362 (3d Cir. 2008).

promoted from a collector to client services representative, support services and consumer resolution team lead, assistant manager, compliance manager, and finally, in 2021, she was promoted to senior manager of compliance services. (*Id.* ¶¶ 431–49.) Badaczewski began working for NRA on September 14, 2020, as a marketing employee. (*Id.* ¶¶ 160, 189.)

A. Facts Relating to Claims Alleged in NRA's Amended Complaint

NRA has multiple layers of security for its computer system, including firewalls, policies against working from home without a company-issued laptop and VPN, multi-factor authentication, and policies against accessing the computer system from personal devices. (*Id.* ¶¶ 6–12.) Further, NRA's security manual prohibits sharing login IDs and passwords or imitating another user. (*Id.* ¶¶ 19, 20.) NRA's security manual also forbids storing passwords "in readable form, in printable or written form or in any location where unauthorized personnel might discover them." (*Id.* ¶ 22.) NRA also has customer privacy policies, Fair Debt Collection Practices Act ("FDCPA") and Health Insurance Portability and Accountability Act ("HIPAA") policies, and workplace policies that prohibit using company computers for personal use. (*Id.* ¶¶ 30–37.) NRA has confidentiality policies, e-mail usage policies, and internet usage policies, which both Defendants acknowledged at the time of their hire. The policies contain possible consequences for violations, including termination. (*Id.* ¶¶ 171–208.)

It is undisputed that both Defendants were aware, generally, of all of these policies, due to the signed declarations they executed at the beginning of their employment. They also admitted multiple times in depositions that they were aware of such policies. (Doc. 174.)

Durenleau was out of the office from January 4, 2021, through January 13, 2021, on COVID leave. (*Id.* ¶ 50.) Durenleau was not given a company computer to access the computer system at home and could only access her company e-mail account through her personal cell phone. (*Id.* ¶¶ 43, 46.) Durenleau was denied a laptop and access to the physical office while on COVID leave. (*Id.* ¶¶ 52, 53.)

On the morning of January 6, 2021, Durenleau's supervisor, Lisa Daube, discovered that there was an issue with one of NRA's state licenses that needed to be resolved that day. (*Id.* ¶¶ 62, 67.) The issue required logging in to the National Multistate Licensing System & Registry ("NMLS"). (*Id.* ¶ 71.) Durenleau controlled portions of NMLS on behalf of NRA. (*Id.* ¶ 74.) Daube called Durenleau to ask for her username and password to NMLS. (*Id.* ¶ 75.) Durenleau told Daube she did not remember her password. (*Id.* ¶ 79.) Through text messages, Daube asked Durenleau "can you resend Steve's [Kusic] access to NMLS?" and also wrote "I can have Doug sift your emails or you can share your log on so we can pay this today." (*Id.* ¶¶ 93, 94.)

Throughout the morning of January 6, when Durenleau was attempting to assist her superiors in dealing with this issue, she was texting and calling Badaczewski, who was at her office. (*Id.* at ¶¶ 82–95.) Durenleau provided Badaczewski with her log on information to the NRA computer, Badaczewski logged in as Durenleau from her (Badaczewski's) computer, and Badaczewski accessed a spreadsheet in Durenleau's files containing Durenleau's passwords. (*Id.* ¶¶ 103–106.) Three minutes after the phone call with Badaczewski, Durenleau relayed her NMLS credentials to Daube. (*Id.* ¶ 107.)

On the afternoon of January 6, 2021, Kusic sent Durenleau various emails about this issue. At 12:20 pm, Kusic wrote,

> We have a major compliance issue and it needs to be resolved today. I can not figure out how to use NMLS in a short period of time. Please let me know how YOU are going to get this fixed by the end of business today. A reminder this is outstanding since December 16th.

(Doc. 162-1, p. 7.)

At 12:37 pm Durenleau responded, "I went on to NMLS I don't see anywhere to pay anything. I don't have the papers. I am not sure what to do from home." (*Id*. at 8.) At 12:42 p.m., Kusic responded with the various outstanding documents and also wrote "[t]his is outstanding since December 16th, it must be finalized by the end of business today. How you do it, is your problem." (*Id.*) Less than a minute later, Durenleau responded "[a]ll of these were uploaded on Wednesday." (*Id.* at 9.) Kusic responded one minute later, "[t]he system says they

are outstanding, as of today. I am not learning NMLS today, get this License Renewed TODAY!!!" (*Id.* at 9 (emphasis in original).) The issue was resolved by 2:14 pm. (Doc. 174, ¶ 122.)

On January 7, 2021, Badaczewski again logged in as Durenleau and emailed the spreadsheet containing Durenleau's passwords to Durenleau's personal email account and then to her work email account. (*Id.* ¶¶ 139, 155.) The password spreadsheet contained "usernames, passwords and other credentials" for the various web portals that NRA used in its debt collection business. (*Id.* ¶ 219.) These portals contain personal information of consumers "including names, dates of birth, social security numbers, utility bills, medical bills, financial account information, and other information." (*Id.* ¶ 220, 228.)

The spreadsheet also contained NMLS credentials for Durenleau, Kusic, and his wife, Jill Kusic.[2] (*Id.* ¶ 317.) These credentials allow access to a portal containing personal information regarding the Kusics, such as social security numbers, dates of birth, address, telephone, e-mail, background checks and credit reports. (*Id.* ¶ 322.)

[2] Jill Kusic is a co-owner and head legal counsel of NRA. (*Id.* ¶ 316.)

On January 22, 2021, Durenleau sent an e-mail to supervisors at NRA regarding moving accounts out of the compliance "workgroup."[3] (*Id.* ¶ 361.) This email prompted her supervisor, Lisa Daube, to ask Durenleau what she meant by the email. (*Id.* ¶ 362.) The two had a meeting where Durenleau explained her concerns and gave an example. (*Id.* ¶¶ 364, 365.) Daube did not agree with the concern Durenleau raised or her example of moving accounts. (*Id.* ¶ 366.)

NRA conducted an audit of account movement in January 2021. (*Id.* ¶ 367.) Anita Schaar ("Schaar"), Director of Internal Controls, performed the audit. (*Id.* ¶¶ 367–69.)[4] The audit showed that Durenleau moved 146 accounts that month, and eleven had been moved after payment was received. (*Id.* ¶¶ 382, 383.) This troubled Schaar because she believed there was no further work to be done on these accounts, and by moving them, Durenleau would be credited for a bonus on an account that had no further work to be done. (*Id.* ¶ 378, 381.) However, Durenleau testified there could be additional work done after payment was received. (Doc. 161-7, pp. 35–36.)[5] Durenleau testified she did work on these

[3] "NRA uses workgroups to identify whether a collection action belongs to a specific employee for purposes of bonuses and commissions." (*Id.* ¶ 345.) In order to receive a bonus at NRA, an employee had to "do something" on an account. (*Id.* ¶ 343.) What exactly this "something" amounts to is unclear from the record. It is undisputed that Durenleau moved accounts into her "workgroup" so that she could receive a bonus regarding these accounts. (*Id.* ¶¶ 352, 353.)

[4] Schaar's credibility is disputed because she does not have firsthand knowledge of how bonusing works at NRA. (*Id.* ¶¶ 377–84.)

[5] For ease of reference, the court utilizes the page numbers from the CM/ECF header.

accounts and moving these accounts was permitted because she had different "ground rules" than the collectors. (Doc. 161-7, p. 34; Doc. 161-19, p. 33; Doc. 162-15.) While Schaar was performing the audit, Durenleau called Schaar asking if she did something wrong. (Doc. 174, ¶ 387.) Various employees testified that they considered what Durenleau did to be fraud and/or theft. (*Id.* ¶¶ 390–397.) Durenleau moved a total of $3,042.85 in payments in January 2021. (*Id.* ¶ 358.) Durenleau received a corrective action on February 2, 2021, outlining the allegedly fraudulent activity, and warning Durenleau that she would be terminated with her next violation, but she was not terminated at that time. (*Id.* ¶¶ 758–60.)

B. Facts Relating to Durenleau's Harassment Claims

Within one year of her hire in 2014, in a one-on-one meeting in a conference room, Kusic "suggested that Kusic and Durenleau picture each other naked to assist with Durenleau's fear of public speaking." (Doc. 174, ¶ 461.) Kusic made comments multiple times to Durenleau, stating "oh here's the blonde again" and "I'm talking to a blonde," referencing her hair color at the time and implying she was dumb. (*Id.* ¶ 462.) Around 2016 or 2017, Kusic referenced another employee who went skinny dipping with him and speculated whether Durenleau would do the same. (*Id.* ¶¶ 467, 568.) Durenleau immediately reported this comment to Sharma, who took no action regarding it. (*Id.* ¶ 469.)

Sometime between 2014 and 2016, Tasey Leitzell, an HR employee, Schaar, and Sharma joked in Durenleau's presence that Durenleau should sleep with Kusic so that Kusic would stop bothering them. (*Id.* ¶¶ 475, 476.) Durenleau responded to this statement by laughing and stating "that would be disgusting[,]" "[he] can't afford me[,]" and "I would never take anything from [Kusic] to blow him or to screw him." (*Id.* ¶¶ 481–83.)

Between 2016 and 2019, Kusic asked Durenleau "how well does your man have it at home." (*Id.* ¶ 486.) Sometime in 2017 or 2018, Kusic wiped a cheese curl over Durenleau's lips and gave her a "funny look." (*Id.* ¶ 492.) In 2019, there was a malware incident at NRA and employees openly speculated that it was because Kusic was watching pornography in his office. (*Id.* ¶ 499.)

On an unspecified date, Sharma relayed comments to Durenleau that other people were making about her clothing. (*Id.* ¶ 504.) The content of these comments is disputed, as NRA, Kusic, and Sharma characterize the comments as Sharma telling Durenleau that an HR employee thought her "pants were too tight or her skirt was too short," and Durenleau claims Sharma told her "how [she was] a whore and, you know, your pants are too tight, or your skirt's too short." (*Id.* ¶ 504.)

In 2015 or 2016, Sharma made several comments regarding another employee's weight including that she focused on food more than work, that this

employee's desk would need cleaned from being full of food and made faces insinuating this employee was fat. (*Id.* ¶¶ 511–16.) Sharma made multiple comments during Durenleau's employment about how large a female employee's breasts were. (*Id.* ¶ 529–26.)

Throughout Durenleau's entire employment at NRA, fellow employee Tasey Leitzell would comment loudly in her office "[i]f these trifling bitches would learn how to swallow, we wouldn't have to pay for their welfare[]" and "I'm so over this job; having to clean the bathroom up after people; and then bitching about their welfare." (*Id.* ¶¶ 552–53.)

In 2020, Sharma made comments in Durenleau's presence about a female employee he was sexually interested in. (*Id.* ¶ 528.) Also in 2020, after Durenleau interviewed Badaczewski, Durenleau, Sharma, and the head of HR met regarding whether they should hire Badaczewski. (*Id.* ¶¶ 543, 546.) During this meeting, one of the two men commented that Badaczewski was the type of girl Kusic liked. (*Id.* ¶ 548.) In response, Durenleau stated, "you guys are gross [. . .] I could get her before you." (*Id.* ¶ 549.) Either Sharma or the head of HR requested that Durenleau record any sexual relations between her and Badaczewski and send it to them. (*Id.* ¶ 550.)

Durenleau testified that every day Sharma would put his arm around her hip or shoulder in greeting. (*Id.* ¶¶ 561–62.) He also gave her shoulder and neck rubs.

(*Id.* ¶ 565.) Once, while Sharma had his arm around Durenleau, he "brushed down [Durenleau's] back and brushed over [her] butt." (*Id.* ¶ 567.) Durenleau did not tell Sharma not to hug her, but she did report this incident to HR. (*Id.* ¶ 566.)

On November 20, 2020, Durenleau was in her office with several of her direct reports on speaker phone with a co-worker in another office building who was complaining about a different co-worker. (*Id.* ¶¶ 577, 579.) Sharma walked down the hall and witnessed the end of the conversation. (*Id.* ¶ 582.) Sharma then entered Durenleau's office, directed her direct reports to leave, and closed the door. (*Id.* ¶ 586.) While discussing the appropriateness of criticizing other co-workers in front of her direct reports, Sharma slapped Durenleau on the face. (*Id.* ¶¶ 595.) He then said "I'll take care of it on Monday" and abruptly left. (*Id.*)

Durenleau reported the incident to in-house counsel later that day, who advised her to write everything down. (*Id.* ¶¶ 597–98.) Durenleau handwrote a statement that night and then emailed it to in-house counsel on Monday. (*Id.* ¶¶ 600–01.) After receiving the statement, in house counsel emailed Durenleau theorizing that this complaint arose from Durenleau feeling insecure in her job and suggested how "a feeling of job insecurity could lead to 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." (Doc. 174-8, p. 2.) Durenleau reported this incident to the Camp Hill Police on February

25, 2021. (*Id.* at ¶ 641.) Sharma was convicted of criminal harassment on May 6, 2021. (Doc. 143, ¶ 170.)

Durenleau resigned from NRA on February 21, 2021, and took a position as a permitting and licensing manager at West Shore Homes. (Doc. 174, ¶ 779.) In her resignation letter Durenleau stated,

> I have been targeted and harassed at NRA Group, LLC for some time now. The harassment was taken to a whole new level when Shell Sharma slapped me across my face the end of November last year. Ever since I made my complaint, I have been targeted to force me out of my job. Emotionally, I cannot take this any more, and am therefore resigning to free myself from this environment.

(Doc. 161-9, p. 16.)

C. Facts relating to Badaczewski's Harassment Claims[6]

Badaczewski testified that she was subjected to sexual harassment "all day, every day" during her employment at NRA, estimating there was at least 120 incidents. (Doc. 174, ¶ 829.) On one occasion, Kusic told Badaczewski that men liked her because she had big boobs and blonde hair. (*Id.* ¶ 833.) Kusic frequently questioned her intelligence, referencing her blonde hair. (*Id.* ¶ 834.) Badaczewski and Kusic would discuss Badaczewski's sex life, and Kusic would comment on it. (*Id.* ¶ 836.) Badaczewski testified in an interview with a detective related to this

[6] The court notes that Plaintiff alleges a multitude of other facts regarding Badaczewski's character, such as facts showing that Badaczewski has a "drinking problem" due to her texting Kusic while intoxicated and her criminal record reflecting a public intoxication charge. . The court is not including the extraneous facts alleged by Plaintiff in this section because they have no bearing on the resolution of the pending motions.

case, "he never touched me, he never made advances at me. But he made comments about, like, my body and me having sexual intercourses with men." (Doc. 162-7, p. 19.) On January 28, 2021, Badaczewski emailed HR regarding Kusic being condescending, not training her, and insulting her intelligence, and she also told other supervisors that Kusic was "constantly talk[ing] about me being blonde and having big boobs." (Doc. 161-13, pp. 24–25; Doc. 174, ¶ 866.) Badaczewski allegedly kept a notebook containing all of the incidents of sexual harassment, but she no longer knows where that notebook is. (Doc. 174, ¶¶ 875–82.)

On March 19, 2021, Badaczewski and Kusic took a trip to two local candy stores in order to buy candy for clients and an office event. (*Id.* ¶ 889.)[7] On this trip, Kusic bought Badaczewski candy and then asked if other guys buy her as many gifts as he does. (Doc. 161-11, p. 220.) While they were on this trip, personnel at NRA discovered that Badaczewski had been the person to log in to Durenleau's account on January 6 and 7. (Doc. 174, ¶ 901.) Upon his return to the office, Kusic became aware of this fact and decided to terminate Badaczewski's employment. (*Id.*) Badaczewski's desk was emptied the next day, March 20,

[7] Plaintiff's counsel quibbles that Badaczewski "falsely" alleged the two went to "Hershey Park" when they actually went to "Hershey's Chocolate World." (Doc. 161-4, p. 124.) The court notes that these two locations are next to each other, share a parking lot, and can be referenced collectively.

2021. (*Id.* ¶ 910.) Badaczewski arrived at the office that day and was presented a corrective action report which terminated her employment. (*Id.* ¶ 915.)

D. Procedural History

NRA filed the initial complaint on April 16, 2021, which named only Durenleau as a defendant, alleging one count of violation of the CFAA. (Doc.1.) On May 19, 2021, NRA filed an amended complaint adding Badaczewski and three more CFAA claims, a violation of the Defend Trade Secrets Act ("DTSA"), a violation of the Pennsylvania Uniform Trade Secrets Act ("PUTSA"), a civil conspiracy claim, a breach of common law duty of loyalty claim, and a fraud claim against Durenleau only. (Doc. 8.) Thereafter, on June 18, 2021, Durenleau answered the complaint and raised counterclaims against NRA including a claim of negligent hiring and retention, alleging various inappropriate comments made by NRA employees and the slap incident with Sharma. (Doc. 16.) On July 20, 2021, Badaczewski answered the complaint, raising one count of sexual harassment under Title VII, one count of quid pro sexual harassment under Title VII, and one count of retaliation under Title VII. (Doc. 24.)

On July 28, 2021, Durenleau filed an amended answer, alleging one count of sexual harassment under Title VII, one count of quid pro sexual harassment under Title VII, and one count of retaliation under Title VII. (Doc. 25.) NRA answered Badaczewski's counterclaims on August 10, 2021. (Doc. 31.) NRA answered

Durenleau's counterclaims on August 17, 2021. (Doc. 33.) Over one year of highly contentious discovery followed.

Durenleau and Badaczewski were granted leave to amend their counterclaims on November 10, 2022. (Doc. 141.) Thereafter, on November 10, 2022, both Durenleau and Badaczewski filed amended answers with counterclaims, adding Kusic and Sharma as counterclaim defendants by adding PHRA claims which mirrored the Title VII claims but also alleged individual liability. (Docs. 142, 143.) NRA, Kusic, and Sharma answered the amended counterclaims on November 23, 2022. (Docs. 144, 145.)

The parties filed simultaneous motions for summary judgment on May 15, 2023. (Docs. 158, 161.) Both motions have been fully briefed and are now ripe for disposition.

JURISDICTION AND VENUE

This court has jurisdiction under 28 U.S.C. §§ 1331 because all parties bring claims arising from federal statutes. This court also has supplemental jurisdiction over state law tort and PHRA claims under 28 U.S.C. § 1367 because the state law claims are sufficiently related to the federal claims. Venue is appropriate under 28 U.S.C. § 1391 because all actions or omissions alleged occurred in the Middle District of Pennsylvania.

STANDARD OF REVIEW

A court may grant a motion for summary judgment when "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A dispute of fact is material if resolution of the dispute "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Summary judgment is not precluded by "[f]actual disputes that are irrelevant or unnecessary." *Id.* "A dispute is genuine if a reasonable trier-of-fact could find in favor of the nonmovant' and 'material if it could affect the outcome of the case." *Thomas v. Tice*, 943 F.3d 145, 149 (3d Cir. 2019) (quoting *Lichtenstein v. Univ. of Pittsburgh Med. Ctr.*, 691 F.3d 294, 300 (3d Cir. 2012)).

In reviewing a motion for summary judgment, the court must view the facts in the light most favorable to the non-moving party and draw all reasonable inferences in that party's favor. *Jutrowski v. Twp. of Riverdale*, 904 F.3d 280, 288 (3d Cir. 2018) (citing *Scheidemantle v. Slippery Rock Univ. State Sys. of Higher Educ.*, 470 F.3d 535, 538 (3d Cir. 2006)). The court may not "weigh the evidence" or "determine the truth of the matter." *Anderson*, 477 U.S. at 249. Instead, the court's role in reviewing the facts of the case is "to determine whether there is a genuine issue for trial." *Id.*

The party moving for summary judgment "bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of 'the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any,' which it believes demonstrate the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986) (quoting Fed. R. Civ. P. 56(c)). The non-moving party must then oppose the motion, and in doing so "'may not rest upon the mere allegations or denials of [its] pleadings' but, instead, 'must set forth specific facts showing that there is a genuine issue for trial. Bare assertions, conclusory allegations, or suspicions will not suffice.'" *Jutrowski*, 904 F.3d at 288–89 (quoting *D.E. v. Cent. Dauphin Sch. Dist.*, 765 F.3d 260, 268–69 (3d Cir. 2014)).

Summary judgment is appropriate where the non-moving party "fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex*, 477 U.S. at 322. "The mere existence of a scintilla of evidence in support of the plaintiff's position will be insufficient; there must be evidence on which the jury could reasonably find for the plaintiff." *Anderson*, 477 U.S. at 252. "Where the record taken as a whole could not lead a rational trier of fact to find for the non-moving party, there is no genuine issue for trial." *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

DISCUSSION

The court will first address NRA's claims against Durenleau and Badaczewski, on which there are competing motions for summary judgment. The court will then review Durenleau's and Badaczewski's counterclaims, on which NRA, Kusic, and Sharma have moved for summary judgment.

A. NRA's Claims against Durenleau and Badaczewski

The court will begin with Durenleau and Badaczewski's motion for summary judgment because the court's resolution of their motion will resolve each of these claims. Durenleau and Badaczewski argue that there is no evidence supporting any of NRA's claims, which entitles them to judgment as a matter of law. (Doc. 160.) Conversely, NRA argues they are entitled to judgment as a matter of law because the facts underlying all of the claims in their amended complaint are undisputed. (Doc. 172.)

1. Computer Fraud and Abuse Act Claims

NRA brings four claims of computer fraud under the CFAA all relating to the incident on January 6 and 7, 2021 when Durenleau was asked by her superiors to resolve a work issue while out of the office on COVID leave, without access to a work computer.[8] It is undisputed that Durenleau asked Badaczewski to access

[8] Count 1 alleges a violation of 18 U.S.C. § 1030(a)(2)(C). (Doc. 8.) Count 2 alleges a violation of 18 U.S.C. § 1030(a)(4). (*Id.*) Count 3 alleges a violation of 18 U.S.C. §1030 (a)(5)(c). (*Id.*) Count 4 alleges a violation of 18 U.S.C. § 1030 (a)(6). (*Id.*)

Durenleau's desktop to send Durenleau her passwords in order to enable Durenleau to resolve this issue. Durenleau and Badaczewski argue there is no evidence showing they exceeded their authorized access in violation of the CFAA because they were both authorized to access NRA's computer systems by virtue of their employment, Durenleau's position as compliance manager, and the implicit demands by supervisors to complete this task. (Doc. 160, pp. 12–17.) They also argue that there is no evidence of intent to defraud under subsections (a)(4) and (a)(6). (*Id.* at 17–19.) NRA responds that neither Durenleau nor Badacezwski were authorized to access the NRA computers because they were not authorized to access the NRA computer system from their homes, and Badaczewski's entry into Durenleau's desktop was unauthorized access in contravention of NRA computer and security policies. (Doc. 172, pp. 8–13.)

The purpose of the CFAA is to "address the growing problem of computer hacking, recognizing that, '[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as how to break into that computer system.'" *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012); *see also Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 61, 613–14 (E.D. Pa. 2013) (analogizing the limitations of the CFAA as akin to burglary). Additionally, courts within this Circuit have cautioned that:

> The CFAA "remains primarily a criminal statute designed to combat hacking," and, as such, jurisprudential care should be taken not to

> "contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to [defendants] who access computers or information in bad faith."

Christian v. Lannett Co., No. 16-963, 2018 U.S. Dist. LEXIS 52793, at *16 (E.D. Pa. Mar. 29, 2018) (quoting *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 590 (E.D. Pa. 1990)). With this background and purpose in mind, the court turns to the claims at hand.

Because it is the broadest subsection, the court starts with Count III, alleging a violation of 18 U.S.C. § 1030(a)(5)(C), which provides, "[w]hoever . . . (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss . . . shall be punished as provided in subsection (c) of this section." While "authorization" under the CFAA has not yet been defined by the Third Circuit, courts within the circuit have explained that "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) (quoting *Dresser–Rand*, 957 F. Supp. 2d at 617). Further, "those who have permission to access a computer for any purpose, such as employees, cannot act 'without authorization' unless and until their authorization to access the computer is specifically rescinded or revoked." *QVC, Inc.*, 159 F. Supp. at 595.

Indeed, "an employee granted access to a computer in connection with his [or her] employment is 'authorized' to access that computer under the CFAA regardless of his or her intent or whether internal policies limit the employee's use of the information accessed." *ClinMicro Immunology Ctr., LLC v. PrimeMed, P.C.*, No. 3:11-CV-2213, 2016 U.S. Dist. LEXIS 88774, at *27 (M.D. Pa. July 7, 2016) (collecting cases), *report and recommendation adopted by* 2016 U.S. Dist. LEXIS 99608 (M.D. Pa. July 29, 2016).

It is undisputed that Durenleau and Badaczewski were authorized to access the NRA computer system by virtue of their employment with NRA. (Doc. 159, ¶ 8; Doc. 174, ¶ 161.)[9] Because both Durenleau and Badaczewski were authorized to access the protected computer, there is no violation of 18 U.S.C. § 1030(a)(5)(C), and Durenleau and Badaczewski's motion for summary judgment will be granted as to Count III.

Counts I and II allege violations under §§ 1030(a)(2)(C)[10] and (a)(4),[11] which prohibit unauthorized access as well as exceeding one's authorization. The

[9] NRA's argument that Durenleau was not "authorized" to access her files from home is actually arguing that Durenleau exceeded the authorization given to her by accessing her files in a manner that is proscribed by NRA's computer use policies, as will be explained below.

[10] "Whoever . . . (2) intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains . . . (c) information from any protected computer . . . shall be punished as provided in subsection (c) of this section." 18 U.S.C. § 1030(a)(2)(C).

[11] "Whoever . . . (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the

CFAA defines "exceed[ing] authorized access" as "access[ing] a computer with authorization and [using] 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). The recent Supreme Court case *Van Buren v. United States*, 141 S. Ct. 1648 (2021), sheds light on the appropriate interpretation of "exceeds authorized access." In *Van Buren*, a police officer used a police department database, which he was authorized to access by virtue of his employment, to run a license plate search for someone who had bribed him to do so. *Id.* at 1652. The United States argued the phrase:

> "is not entitled so to obtain" refers to "the information not allowed to [be] obtain[ed] *in the particular manner or circumstances in which he obtained it.* The manner or circumstances in which one has a right to obtain information . . . are defined by any "specifically and explicitly" communicated limits to one's right to access information.

Id. at 1654–55 (emphasis in original). In contrast, Van Buren argued that the statute requires a "gates-up-or-down" inquiry, and that since he was authorized to access the computer, it did not matter that he later used that access in contravention of department policies. *Id.* at 1658–59.

---

intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . shall be punished as provided in subsection (c) of this section." § 1030(a)(4).

The Court adopted Van Buren's argument and reasoned that interpreting "authorization" and "exceeding authorization" to mean "one either can or cannot access a computer system, and one either can or cannot access certain areas within the system[]" aligns better with "the computer-context understanding of access as entry." *Id.* at 1658–59. The Court further disavowed relying on computer use policies as the basis for liability under the CFAA, because "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." *Id.* at 1661.[12]

Here, Durenleau was authorized to access her computer and the files within that computer by virtue of her employment at NRA and having the credentials to access their computer system. NRA's argument that she was not "authorized" to access her computer at home because NRA computer policies forbid such a practice is actually arguing that she exceeded her authorized access by accessing her computer in a prohibited manner. NRA's argument is that: Durenleau's authorization to access the computer was given to her by virtue of her employment; NRA does not allow their employees to use their authorized access in a certain

[12] Other courts have also warned against basing CFAA liability on violations of internal policies because doing so would "allow[] private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law." *Nosal*, 676 F.3d at 860. *See also Carnegie Strategic Design Engineers, LLC v. Cloherty*, No. CIV.A. 13-1112, 2014 WL 896636, at *9 (W.D. Pa. Mar. 6, 2014) ("Plaintiff cannot state a claim under the CFAA by transforming its employee policies which prohibited the using of the computer system for anything other than business purposes into a violation of the CFAA.").

way, i.e. from their homes without specific equipment; and Durenleau accessed her computer in a way not authorized by company policy. Accordingly, accepting NRA's argument that Durenleau exceeded authorized access by accessing the computer in the wrong way would require the court to utilize the definition of "exceeding authorized use" that the Supreme Court rejected in *Van Buren*.

The definitional limitation established in *Van Buren* is particularly significant in light of the purpose of the CFAA. As explained in *Dresser-Rand Co.*,

> An analogy to burglary provides clarity to the limitations of the CFAA: "If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter." Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act,* 13 VAND. J. ENT. & TECH. L. 543, 571 (2011).

Dresser-Rand Co., 957 F. Supp. 2d at 614. Applying this burglary analogy here shows why Badaczewski and Durenleau are not liable under the CFAA. Both had permission to enter the (metaphorical) home. Instead of entering the home through the door, they entered through a window. Conditioning their entry into the home upon only using the door does not make their subsequent entry through the window a burglary. It may be a reason to not invite them back to the home, but it is not a burglary.

Thus, applying the appropriate definition, there is no issue of material fact regarding whether Durenleau was authorized to access the computer system, generally, and her files, specifically. Further, she did not exceed her authorized access by emailing a work document to her personal email. Although these actions may have violated NRA's computer use policies, she was authorized to access those files by virtue of her employment. In other words, Durenleau came in through the window rather than the door, which is not a violation of the CFAA.

Additionally, NRA argues that Badaczewski exceeded her authorization by logging into Durenleau's desktop, accessing the spreadsheet, and emailing it to Durenleau's personal email address because Badaczewski was not authorized to access Durenleau's files. (Doc. 163, p. 40.) NRA argues that no person at NRA explicitly told Durenleau or Badaczewski to take this course of action, and thus, Badaczewski's access of Durenleau's computer was unauthorized. (*Id.* at 34.) While Durenleau was not explicitly told "share your NRA password and let Jamie Badaczewski log in to your computer and send you your passwords," as NRA seems to think the statute requires, the context of this incident shows that Durenleau authorized Badaczewski to access this information.

Durenleau, the senior compliance manager, was at home sick with COVID, when her superiors brought an urgent work issue to her attention. She was denied a company computer to access the computer system at home and could only access

her company e-mail account through her personal cell phone. In order to solve this issue, she needed to give her supervisor a password to an online portal. The CEO of NRA then began emailing Durenleau, emphasizing that she needed to fix the problem by the end of the day and that how she did that was her "problem." Accordingly, in order to perform her job without the necessary computing devices, she authorized her co-worker to access her own files and locate the needed password. The next day, Durenleau directed Badaczewski to send the whole spreadsheet. These circumstances are a far cry from the hacking that the CFAA was enacted to prevent.

While having Badaczewski access Durenleau's desktop and send the password spreadsheet may have been a violation of NRA policies and worthy of an employment sanction, it is not a violation of the CFAA. Therefore, neither Durenleau nor Badaczewski accessed a protected computer without authorization or exceeded their authorization. As a result, Durenleau and Badaczewski's motion for summary judgment will be granted as to Counts I and II.

Count IV alleges a violation of 18 U.S.C § 1030(a)(6), which provides:

> Whoever . . . knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if . . . such trafficking affects interstate or foreign commerce . . . shall be punished as provided in subsection (c) of this section.

In the copious briefing in this case, neither party has provided the court with a definition of "intent to defraud" as used in the CFAA. However, other courts have held that, under the CFAA, an intent to defraud "only requires a showing of unlawful access; there is no need to plead the elements of common law fraud to state a claim under the Act." *eBay Inc. v. Digital Point Sols., Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (citing *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008)).

NRA's argument regarding whether Durenleau and Badaczewski had an intent to defraud consists of restating its allegations that Durenleau and Badaczewski were not authorized to take these actions, pointing to Durenleau's statement that giving her NMLS credentials to her supervisor would have been "dumb" because her supervisor did not like her, arguing that Badaczewski's access to Durenleau's desktop exceeded Badaczewski's authorized access, and arguing that sending the password spreadsheet in an unencrypted email shows Durenleau and Badaczewski "knowingly and intentionally exposed the confidential information [NRA] is entrusted with protecting, but did so with the clear intent to use the information to cause [NRA] financial and reputational harm." (Doc. 172, pp. 17–19.) NRA also attempts to support their assertion that Durenleau or Badaczewski further disseminated the spreadsheet by pointing to testimony of Sharma, where he speculates that NRA losing their $10 million cyber insurance

coverage six months after the incident was due to the emailed spreadsheet because Durenleau was one of the only people who knew of this coverage and that a recent fraudulently filed unemployment claim under Kusic's name was due to the personal information contained in the spreadsheet. (*Id.* at 18.)

As explained above, Durenleau and Badaczewski did not unlawfully access NRA's computers. There is no further evidence in the record, beyond Sharma's unsubstantiated speculation, showing an intent to defraud NRA in any way. Speculations are not sufficient to support summary judgment, and therefore, Durenleau and Badaczewski's motion for summary judgment will be granted as to Count IV. *See Jutrowski v. Twp. of Riverdale*, 904 F.3d 280, 288–89 (3d Cir. 2018).

2. Trade Secrets Claims

NRA brings one count of violating the DTSA[13] and one count of violating the PUTSA[14] on the premise that the password spreadsheet allowed access to the multiple online portals utilized by NRA, which contain personal and confidential information of its customers and consumers. (Doc. 172, p. 20.) Durenleau and Badaczewski argue that the password spreadsheet does not contain trade secrets because the passwords do not have independent economic value. (Doc. 160,

[13] 18 U.S.C. § 1836.

[14] 12 PA. CON. STAT. § 5306.

p. 20.) NRA responds that the password spreadsheet is a trade secret because the passwords on that spreadsheet would allow access to a "myriad" of customers' personal information which has value to cyber criminals. (Doc. 163, p. 49.)

Because the DTSA and PUTSA protect the same type of information, the court will consider these claims together. *PharMerica Corp. v. Sturgeon*, No. 2:16-CV-1481, 2018 WL 1367339, at *4 (W.D. Pa. Mar. 16, 2018). Under both the DTSA and PUTSA, a trade secret is "information that: (a) the owner has taken reasonable means 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) others who cannot readily access it would obtain economic value from its disclosure or use." *Id.* at *4.

> To determine whether information is a trade secret, a court must consider:
>
> > the extent to which the information is known outside of the owner's business, the extent to which it is known by employees and others involved in the owner's business, the value of the information to the owner and his competitors, the amount of effort or money expended in developing the information, and the ease or difficulty with which the information could be acquired or duplicated by others. *S.I. Handling Systems, Inc. v. Heisley,* 753 F.2d 1244, 1256 (3d Cir.1985).

Crown Coal & Coke Co. v. Compass Point Res., LLC, No. CIVA 07-1208, 2009 WL 891869, at *6–7 (W.D. Pa. Mar. 31, 2009)*; see also Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102, 109 (3d. Cir. 2010).

Additionally, "[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 (E.D. Pa. 2014). Further, "compilation of customer data may qualify as a trade secret if it is not readily obtainable from another source and 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).

Durenleau and Badaczewski rely on *State Analysis, Inc. v. American Financial Services Association*, 621 F. Supp. 2d 309 (E.D. Va. 2009), for their argument that passwords cannot be trade secrets. In *State Analysis*, defendant, a former customer of plaintiff, shared its passwords which accessed plaintiff's databases, with one of plaintiff's competitors. *State Analysis*, 621 F. Supp. 2d at 314. The court held that passwords themselves are not information but rather are a barrier to the information which is properly called a trade secret. *Id.* at 321. The court further reasoned that "[a]lthough the passwords at issue clearly have economic value . . . , they have no *independent* economic value in the way a formula or a customer list might have." *Id.* (emphasis in original).[15]

[15] NRA distinguishes this case by arguing that it applies the Virginia trade secrets law. However, as with the Pennsylvania trade secrets law, the Virginia trade secrets law is essentially the same as the federal trade secrets act. Further, the two cases NRA cited to support its argument are both from California and apply the California trade secrets law.

NRA cites two cases for the proposition that passwords can be trade secrets. (Doc. 163, p. 48.) However, both of these cases were decided at the motion to dismiss stage and held that passwords coupled with other information could state a claim for misappropriation of trade secrets. *PhoneDog v. Kravitz*, No. C 11-03474, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011); *TMX Funding, Inc. v. Impero Techs., Inc.*, No. C 10-00202 JF (PVT), 2010 WL 2509979, at *3 (N.D. Cal. June 17, 2010). As such, these cases are not persuasive, and the court will apply *State Analysis*, which is more relevant to the analysis here.

The password spreadsheet has no value outside of the access it gives to the web portals. The information on the web portals themselves may potentially be trade secrets, but that information was not shared and is not at issue here. NRA advances plenty of arguments regarding the various web portals the passwords access and the confidentiality of the information therein, but these arguments do not prove that the passwords have any independent economic value. Rather, these arguments show that the spreadsheet itself has no independent value; the value is in portals that the passwords access. Accordingly, the password spreadsheet has no independent economic value and is not a trade secret. Thus, Durenleau and Badaczewski's motion for summary judgment will be granted as to Counts V and VI.

3. Civil Conspiracy

Durenleau and Badaczewski argue they are entitled to summary judgment on the civil conspiracy claim, Count VII, because there are no facts supporting malicious intent for either of them. (Doc. 160, pp. 23–24.) NRA argues that a conspiracy should be inferred from Durenleau and Badaczewski's communications on January 6 and 7, 2021 when they agreed to violate the CFAA, DTSA and PUTSA. (Doc. 163, p. 65.)

In Pennsylvania, a civil conspiracy requires a showing of "(1) a combination of two or more persons acting with a common purpose to do an unlawful act or to do a lawful act by unlawful means; (2) an overt act done in pursuance of the common purpose; and (3) actual legal damage." *Bro-Tech Corp*, 651 F. Supp. 2d at 418. Moreover, "[p]roof of malice, i.e., an intent to injure, is essential in proof of a conspiracy . . . . Malice requires . . . that the *sole* purpose of the conspiracy was to injure the plaintiff,' and that this intent was without justification." *Synthes*, 25 F. Supp. 3d at 735–36 (quoting *Doltz v. Harris & Assoc.*, 280 F. Supp. 2d 377, 389 (E.D. Pa. 2003)). Finally, a civil conspiracy claim must be based on an underlying tort, and "only a finding that the underlying tort has occurred will support a claim for civil conspiracy. *Id.*

Here, because the court has found that Durenleau and Badaczewski did not violate the CFAA, DTSA, or PUTSA, there can be no civil conspiracy to engage in

some type of unlawful activity. Moreover, there is no evidence in the record demonstrating any intent to harm NRA by their actions on January 6 and 7, 2021. NRA argues that Durenleau and Badaczewski's knowledge of the computer and confidentiality policies, and then their subsequent violation of them, show an intent to injure NRA. (Doc. 172, p. 30.) However, the malice requirement demands that the only purpose of the conspiracy is to injure the plaintiff. *Synthes*, 25 F. Supp. 3d at 736. Here, there is sufficient evidence that Durenleau and Badaczewski were trying to help NRA by resolving the licensing issue, despite not being set up to succeed by NRA. Therefore, Durenleau and Badaczewski's motion for summary judgment will be granted as to Count VII.

4. Breach of Common Law Duty of Loyalty

Durenleau and Badaczewski argue they are entitled to summary judgment on Count VIII, breach of common law duty of loyalty, because there is no evidence that they used the password spreadsheet to compete with NRA. (Doc. 160, p. 26.) NRA argues that creating and sending the password spreadsheet was contrary to NRA's interests, and that Durenleau's alleged mishandling of a license issue was also contrary to NRA's interests. (Doc. 172, pp. 39–42.)

To prove a claim of breach of the common law duty of loyalty in Pennsylvania, a plaintiff must show there was an agency relationship and that:

> [1] the defendant negligently or intentionally failed to act in good faith and solely for the benefit of plaintiff in all matters for which he or she

> was employed; (2) that the plaintiff suffered injury; and (3) that the agent's failure to act solely for the plaintiff's benefit . . . was a real factor in bring[ing] about plaintiff's injuries.

McDermott v. Party City Corp., 11 F. Supp. 2d 612, 626 n.18 (E.D. Pa. 1998).

Further, the agent must:

> refrain from competing with the principal and from taking action on behalf of, or otherwise assisting, the principal's competitors throughout the duration of the agency relationship, as well as . . . not to use property or confidential information of the principal for the agent's own purpose or those of a third party.

Synthes, 25 F. Supp. 3d at 667 (citing RESTATEMENT (THIRD) OF AGENCY §§ 8.04, 8.05).

Here, there is no evidence that Durenleau or Badaczewski used this spreadsheet to compete with NRA at all. As NRA points out, liability for breach of common law duty of loyalty can also be founded upon using the principal's property or confidential information for the agent's own purposes or a third party's. *See* RESTATEMENT (THIRD) OF AGENCY § 8.04. However, there is also no evidence that Durenleau or Badaczewski used the information in any way other than to resolve the licensing issue on January 6, 2021, as requested.

NRA argues that the mere creation and sending of the spreadsheet contrary to NRA policies shows that Durenleau and Badaczewski acted against NRA's interests. However, the evidence of record shows that Durenleau and Badaczewski were acting in NRA's interest by trying to resolve the license issue and did not use

the spreadsheet or the information in it for any other reason than to complete their job duties.

NRA also argues that Durenleau breached her duty of loyalty to NRA by failing to respond to a deficiency notice sent on January 29, 2021, regarding the same license that was the issue on January 6, 2021. (Doc. 172, p. 41.) This issue is raised in the brief supporting NRA's motion for summary judgment and tangentially in the brief in opposition to Durenleau's motion. (Doc. 163, p. 73.) Durenleau argues that this issue is being raised for the first time on summary judgment, and therefore, should not be considered by the court. (Doc. 173, p. 23.) NRA argues that raising this issue for the first time on summary judgment is appropriate because the license at issue is the same one the parties were trying to resolve on January 6, 2021, such that Durenleau had notice that this license was at issue, NRA requested documents in discovery regarding this license, and Durenleau could have questioned Sharma about the license, but chose not to. (Doc. 180, p. 15.)[16]

Third Circuit precedent dictates that "a claim that has not been timely raised is waived." *Spence v. City of Phila.*, 147 Fed. App'x 289, 291 (3d Cir. 2005). The

[16] NRA continuously faults Durenleau and Badaczewski for not addressing the Wyoming license issue in their briefing; however, this issue was not raised as support for the breach of duty of loyalty claim until the summary judgment stage. As the parties filed simultaneous briefs, it is understandable that Durenleau and Badaczewski did not address an argument not yet raised. Durenleau and Badaczewski raise counter arguments in their briefing in opposition to NRA's motion.

Third Circuit has also previously held that a plaintiff should have moved to amend their complaint during discovery when discovery produced evidence of an additional claim. *Josey v. John R. Hollingsworth Corp.*, 996 F.2d 632, 642 (3d Cir. 1993). Here, NRA is not permitted to modify their claims on summary judgment by changing the factual basis for one of the claims. If NRA had wanted to base their breach of duty of loyalty claim on this factual scenario, it could have filed a motion to amend their complaint, as it evidently was aware of this situation as early as February 25, 2021. Accordingly, Durenleau and Badaczewski's motion for summary judgment will be granted on the breach of duty of loyalty claim, Count VIII.

5. Fraud

NRA's final claim is against Durenleau alone and alleges that she committed fraud against NRA by moving certain accounts into her workgroup such that she could receive a bonus based on these accounts. (Doc. 8.) Durenleau argues that there is no evidence showing that she acted with knowledge and intent to defraud. (Doc. 160, p. 27.) NRA responds that she knew the rules for collecting bonuses and moved accounts into her workgroup after payment was made, meaning that she did not perform any work on those accounts entitling her to a bonus. (Doc. 172, p. 44.)

A fraud claim in Pennsylvania law consists of six elements:

> (1) (a) A misrepresentation or (b) A concealment; (2) Which is material to the transaction at hand; (3) (a) Made with knowledge of its falsity or recklessness as to whether it is true or false (for a misrepresentation), or (b) Calculated to deceive (for a concealment); (4) With the intent of misleading another into relying on it; (5) Justifiable reliance on the misrepresentation; and (6) A resulting injury proximately caused by such reliance.

SodexoMAGIC, LLC v. Drexel Univ., 24 F.4th 183, 205 (3d Cir. 2022). Additionally, "[f]raud consists of 'anything calculated to deceive, whether by single act or combination or by suppression of truth, or suggestion of what is false, whether it be by direct falsehood or by innuendo, by speech or silence, word of mouth, or look or gesture.'" *Am. Indep. Ins. Co. v. Lederman*, No. CIV.A. 97-4153, 2000 WL 1209371, at *14 (E.D. Pa. Aug. 25, 2000) (quoting *Moser v. DeSetta,* 589 A.2d 679, 682 (Pa. 1991)).

NRA argues that it was company policy that an employee "do something" on an account in order for them to receive a bonus. It also argues that after the account had closed, there was no more work to do, so no one could then receive a bonus on it. Durenleau allegedly transferred accounts into her work group after they had closed in order for her to receive a bonus off those accounts.

However, Durenleau has presented sufficient evidence that different rules applied to her for receiving a bonus. (Doc. 161-7 p. 34; Doc. 161-19, p. 33; Doc. 162-15, p. 41.) The only evidence NRA presents to show that Durenleau knew that moving these accounts was wrong was when she called Schaar during the audit and

asked whether she did anything wrong. (Doc. 174, ¶ 387.) The court declines to infer from that statement that Durenleau admitted guilt, but rather, that she did not know she was doing something wrong and needed to ask whether she had made a mistake. Accordingly, there is no evidence showing that Durenleau acted with knowledge of any alleged falsity in moving accounts, and she is entitled to summary judgment as a matter of law on Count IX.

In conclusion, there are no genuine disputes of material fact, and Durenleau and Badaczewski are entitled to judgment as a matter of law on the claims raised in the amended complaint. Accordingly, because judgment will be entered in favor of Durenleau and Badaczewski, NRA's motion for summary judgment on the claims brought in the amended complaint will be denied. The court will now consider NRA, Kusic, and Sharma's motion for summary judgment regarding the counterclaims brought by Durenleau and Badaczewski.

B. Durenleau and Badaczewski's Counterclaims Against NRA, Kusic, and Sharma

The court now turns to NRA, Kusic, and Sharma's motion for summary judgment, arguing that there are no genuine disputes of material facts, and they are entitled as a matter of law to judgment in their favor regarding the counterclaims raised against them. (Doc. 163.) Durenleau and Badaczewski argue that there are genuine disputes of material fact regarding their Title VII and PHRA claims. (Doc. 173.) The court draws all reasonable inferences in favor of non-movants,

Durenleau and Badaczewski. Additionally, the court will address the Title VII and PHRA claims together since, "in an action under Title VII and the PHRA, the standards under the federal and state statutes are the same." *Kimes v. Univ. of Scranton*, 126 F. Supp. 3d 477, 491 (M.D. Pa. 2015).

Preliminarily, NRA, Kusic, and Sharma argue that Durenleau and Badaczewski lack standing to bring these claims because at various times in their respective depositions, both Durenleau and Badaczewski stated they are not seeking money from this lawsuit, which shows they have not suffered an injury entitling them to relief. (Doc. 163, p. 83.) As Durenleau and Badaczewski note, these statements instead demonstrate that they are not motivated solely by money in bringing these claims, but they are still seeking monetary damages. (Doc. 142, p. 50.) There has been no amended pleading filed and stray statements in contentious depositions will not deprive Durenleau and Badaczewski of standing. The court will now address the substance of both Durenleau and Badaczewski's claims.

1. Continuing Violation Doctrine[17]

Before filing suit in federal court, a plaintiff must bring a timely charge of discrimination before the EEOC and obtain notice of her right to sue in order to exhaust her administrative remedies. *Mandel v. M & Q Packaging Corp.*, 706 F.3d

[17] This argument is only applicable with respect to Durenleau's claims.

157, 163 (3d Cir. 2013). In order for a charge to be timely, a plaintiff alleging discrimination under Title VII in Pennsylvania must bring an EEOC charge within 300 days after the alleged unlawful employment practice. *See* 42 U.S.C. § 2000e-5(e)(1); *Mikula v. Allegheny Cnty. of Pa.*, 583 F.3d 181, 183 (3d Cir. 2009); *Watson v. Eastman Kodak Co.*, 235 F.3d 851, 854 (3d Cir. 2000). A plaintiff must file a PHRA claim with the Pennsylvania Human Relations Commission within 180 days of the discriminatory act. 43 PA. STAT. § 959(h). Here, Durenleau dual filed her EEOC charge on April 23, 2021; therefore, the limitations period for Title VII began on June 27, 2020, and on October 25, 2020, for the PHRA claims. (Doc. 161-23, p. 2.)

However, the continuing violation doctrine serves as an equitable exception to the time bar under Title VII, allowing courts to consider "discriminatory acts that are not individually actionable . . . so long as they are linked in a pattern of actions which continues into the applicable limitations period." *Mandel*, 706 F.3d at 165 (citing *O'Connor v. City of Newark*, 440 F.3d 125, 127 (3d Cir. 2006)). Therefore, a plaintiff must prove that at least one discriminatory act occurred within the limitations period and that this alleged wrong "is more than the occurrence of isolated or sporadic acts." *Kimes*, 126 F. Supp. 3d at 492. To make this determination, courts may consider subject matter, i.e., "whether the violations constitute the same type of discrimination," *Mandel*, 706 F.3d at 166 n.2, and

frequency, i.e., "whether the acts are recurring or more in the nature of isolated incidents." *Kimes*, 126 F. Supp. 3d at 492. In considering frequency, "courts should consider the time gap between incidents and the number of incidents that have occurred in reaching their conclusion." *Oliver v. Clinical Pracs. of Univ. of Pa.*, 921 F. Supp. 2d 434, 446 (E.D. Pa. 2013). Further, "[a]cts that are taken by two different supervisors, acting independently, over different time periods generally demonstrate isolated events rather than a persistent, ongoing pattern of discrimination." *Id.* at 445.

NRA, Kusic, and Sharma argue that many of Durenleau's allegations are outside the applicable statute of limitations and cannot be used to support her claims of sexual harassment, and the remaining allegations are insufficient to show severe and pervasive harassment as required by Title VII. (*Id.* at 90–105.) Durenleau argues her allegations are timely under the continuing violation doctrine because they show a pattern of harassment.

Durenleau alleges the following actions show a pattern of discriminatory conduct at NRA, beginning in 2014: Kusic suggested they picture each other naked when assisting Durenleau with public speaking; Kusic would comment about Durenleau being blond, insinuating she was stupid; HR employee Tasey Leitzell, Schaar, and Sharma joked about Durenleau sleeping with Kusic so that he would stop bothering them; Sharma made various comments regarding another

employee's weight; unnamed employees joked that Durenleau should be like a former employee who Kusic was obsessed with and allegedly bought a car for; Leitzell, Schaar, Biancha Tatum, and Kira West joked about "cleaning up the mess after;" Kusic insinuated he wanted to go skinny dipping with Durenleau; Kusic asked Durenleau "how well does your man have it at home;" Kusic swiped a cheese curl over Durenleau's lips and gave her a funny look; it was rumored in the office that a malware incident was due to Kusic watching porn in his office; Sharma discussed with Durenleau how another employee wanted to sleep with him; Sharma stated in Durenleau's presence that he wanted to sleep with another employee; after Jamie Badaczewski's employment interview, Sharma and the HR director told Durenleau that if she and Badaczewski had sex, they should film it and send it to the two men; on unspecified dates, HR employee Tasey Leitzell used to make derogatory comments regarding the collection employees; at various times throughout her employment, Durenleau and Sharma would give each other neck rubs; on an unspecified date, Sharma told Durenleau another employee had an issue with her clothes, relaying the employee said Durenleau was a "whore" and that her clothes were too tight and short; on an unspecified date, Sharma made comments about another employee's breasts; and Sharma would greet Durenleau every day with a hug or arm around the shoulder. Finally, Durenleau argues this

pattern of sexual harassment culminated with Sharma slapping her on November 20, 2020.

Here, Durenleau has provided evidence that one act occurred during the limitations period: the November 2020 slap by Sharma. Next, she has shown an ongoing practice of discrimination. Although not all overtly sexual, Durenleau alleges many inappropriate sexual and sex-based comments as well as multiple instances of inappropriate touching which could be interpreted by a reasonable jury to show a pattern of sexual harassment by Kusic and Sharma. The incidents mostly involve Durenleau's only two supervisors at NRA: Kusic and Sharma. While the events were perpetrated by two different supervisors at two distinct time periods, a reasonable jury could still connect the actions of these supervisors as one larger pattern because both men were in upper management at NRA and as such, were responsible for fostering an environment where this type of behavior was condoned. Events that do not involve either Kusic or Sharma, such as Ms. Leitzell's general comments about the collection floor, will be excluded from consideration. Additionally, Durenleau's gender could be a substantially motivating factor for the incidents because many of the comments dealt with her sex life. A reasonable jury could find that Kusic and Sharma would not have treated a male employee the same way. In total, the incidents were also fairly frequent, with a total of 15 incidents over 6.5 years and some occurring on a daily

basis. Accordingly, the court will consider the events involving either Kusic or Sharma in analyzing whether NRA, Kusic, and Sharma are entitled to summary judgment on the hostile work environment claim.

2. Durenleau and Badaczewski's Hostile Work Environment Claims

i. Durenleau's Hostile Work Environment Claim

Title VII makes it "an unlawful employment practice for an employer . . . to discriminate against an individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, sex, or national origin." 42 U.S.C. § 2000e-2(a)(1). Sexual harassment is discrimination based on one's sex. *Meritor Savings Bank, FSB v. Vinson*, 477 U.S 57, 65 (1986). Sexual misconduct, such as "[u]nwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature . . ." constitutes sexual harassment "whether or not it is directly linked to the grant or denial of an economic *quid pro quo*, where 'such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.'" *Id.* (quoting 29 CFR § 16041.11(a)(3)).

In order to state a claim for a hostile work environment, an employee must show "(1) the employee suffered intentional discrimination because of [her] sex, (2) the discrimination was pervasive and regular, (3) the discrimination

detrimentally affected the [employee], (4) the discrimination would detrimentally affect a reasonable person of the same sex in that position, and (5) the existence of *respondeat superior* liability." *Andreoli v. Gates*, 482 F.3d 641, 643 (3d Cir. 2007).

First, the "[o]ffensive conduct need not necessarily include obvious sexual overtones in order to constitute unlawful harassment or discrimination." *Hargrave v. Cnty. of Atl.*, 262 F. Supp. 2d 393, 412 (D.N.J. 2003) (citing *Andrews v. City of Phila.*, 895 F.2d 1469, 1485 (3d Cir. 1990)). Instead, only "a showing that [plaintiff's gender was] a substantial factor in the harassment, and that if the plaintiff had been [male] she would not have been treated in the same manner[]" is required. *Aman v. Cort Furniture Rental Corp.*, 85 F.3d 1074, 1083 (3d Cir. 1996).

Next, the workplace at issue must be "permeated with discriminatory intimidation, ridicule, and insult that [was] sufficiently severe or pervasive to alter the conditions of [her] employment and create an abusive working environment." *Kimes*, 126 F. Supp. 3d at 498. In determining how severe or pervasive the offensive conduct is, the court must look at the totality of the circumstances, including the "frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it

unreasonably interferes with an employee's work performance." *Harris v. Forklift Sys., Inc.*, 510 U.S. 17, 23 (1993).

Importantly, "[h]ostile environment claims require both an objective and a subjective showing; the environment must have been one that not only a reasonable person would find hostile and abusive, but which the actual Plaintiff in fact found to be hostile and abusive." *Pittman v. Cont'l Airlines, Inc.*, 35 F. Supp. 2d 434, 441 (E.D. Pa. 1999). "A discriminatory abusive work environment, even one that does not seriously affect employees' psychological well-being, can and often will detract from employees' job performance, discourage employees from remaining on the job, or keep them from advancing in their careers." *Harris*, 510 U.S. at 22.

Here, a reasonable jury could find that Durenleau was discriminated against on the basis of her sex. Many of the comments made were directly sexual in nature. The remaining comments were sufficiently related to her gender, such as Kusic referring to her as a blonde or Sharma's comments regarding another employee's weight, that a reasonable jury could find that they would not have been made if Durenleau was a man. Moreover, some of the comments and the slap, while not overtly sexual, were done in a "paternalistic" manner, which brings a level of intimidation that a jury could find would not be used with a man.

Accordingly, a reasonable jury could find that Durenleau was discriminated against based on her sex.

Next, a reasonable jury could find that the conduct was severe and pervasive. Durenleau has alleged and substantiated approximately fifteen incidents over a span of six and a half years. A fair portion of the conduct was in the form of mere utterances or jokes in the office, however, Durenleau does allege and provide evidence that she experienced unwanted touchings in the daily hugs by Sharma, neck rubs, and the slap across the face. There were no overt sexual overtures, but there were several sexual comments directed at her or made about others in her presence. Accordingly, there is a disputed issue of material fact as to how severe or pervasive the conduct was.

We also must consider whether the workplace was hostile and abusive from both an objective and subjective perspective. Here, Durenleau specifically testified that going to work made her uncomfortable and that she had a panic attack in 2018 due to her situation at work. (Doc. 161-8, p. 82.) She also spoke with her therapist about suffering physical and sexual abuse at work. (Doc. 155-1, p. 12.) Durenleau also references the abuse she experienced at NRA as a reason for leaving in her resignation letter, showing that the abusive environment at NRA discouraged her from remaining in employment. This is sufficient to show she subjectively viewed her workplace as hostile and abusive.

Additionally, a reasonable person in the same situation would also find the environment at NRA hostile and abusive. The evidence of record shows an office environment where supervisors freely made inappropriate or sexually charged comments to their staff with no accountability. A reasonable jury could find this environment hostile and abusive.

The final element of a hostile work environment claim is vicarious liability. "An employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee." *Faragher v. City of Boca Raton*, 524 U.S. 775, 807 (1998). When there is no employment action taken, employers may avail themselves of an affirmative defense, where they must show they "exercised reasonable care to prevent and correct promptly any sexually harassing behavior" and "the plaintiff employee unreasonably failed to take advantage of any preventative or corrective opportunities provided by the employer or to avoid harm otherwise." *Id.* This defense is "unavailable when the supervisor in question is the employer's proxy or alter ego." *O'Brien v. Middle East Forum*, 57 F.4th 110, 119 (3d Cir. 2023.) A supervisor is an employer's "proxy" when they are "high enough in the management hierarchy that his actions 'speak' for the employer . . . he may be considered the employer's alter ego." *Id.* at 121.

NRA, Kusic, and Sharma raise a *Faragher/Ellerth* defense by arguing that Durenleau did not utilize the sexual harassment complaint system NRA had in place. (Doc. 163, pp. 105–10.) Durenleau argues that the *Faragher/Ellerth* defense is inapplicable in this case because the two people she is alleging sexually harassed her are proxies for NRA. (Doc. 176, p. 98.)

Here, there was no employment action taken against Durenleau because she resigned. It does not appear that Kusic was ever Durenleau's direct supervisor, although at all times he was the CEO. Sharma was either her immediate supervisor or a successively higher supervisor and also the COO. (Doc. 174, ¶ 411.) Kusic and Sharma are proxies of NRA because they are sufficiently high in the management structure that their actions could be said to speak for NRA. Therefore, the *Faragher/Ellerth* defense is unavailable, and NRA is subject to vicarious liability. In conclusion, there are disputed issues of material fact such that a jury must decide these questions. NRA, Kusic, and Sharma's motion for summary judgment as to Counts I and IV of Durenleau's counterclaims will be denied.

ii. Badaczewski's Hostile Work Environment Claim

NRA, and Kusic only raise the *Fargher/Ellerth* defense arguing that Badaczewski did not utilize the sexual harassment complaint system NRA had in

place. (Doc. 163, p. 131.)[18] As noted above, the *Faragher/Ellerth* defense is not available to employer proxies. As Kusic was Badaczewski's direct supervisor and CEO, a reasonable jury could find that he was a proxy of NRA. Therefore, NRA is subject to vicarious liability for Badaczewski's hostile work environment count, Counts I and IV, and Kusic's motion for summary judgment on Badaczewski's hostile work environment claim will be denied.

3. Quid Pro Quo Sexual Harassment

The Third Circuit has adopted the test set out by 29 C.F.R. § 1604.11(a)(1) and (2) for the elements of a quid pro quo sexual harassment claim, which provides:

> Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when (1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment [or] (2) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual . . . .

29 C.F.R. § 1605.11(a)(1), (2).

An employee does not need to be threatened with or experience economic or tangible discrimination, but the "sexual advances must be sufficiently severe as to

[18] The court notes that there is no evidence in the voluminous record of when Badaczewski filed her EEOC charge. There is evidence that Badaczewski received a right to sue letter on June 29, 2021. (Doc. 24-4, p. 2.) However, NRA does not dispute the timeliness or even the substance of Badaczewski's hostile work environment claim. Accordingly, that count will proceed past summary judgment.

alter the employee's 'compensation, terms, conditions or privileges of employment,' or to 'deprive or tend to deprive [him or her] of employment opportunities or otherwise adversely affect his [or her] status as an employee.'" *Robinson v. City of Pittsburgh*, 120 F.3d 1286, 1296 (3d Cir. 1997) (citing 42 U.S.C. §§ 2000e-2(a)(1), (2)). The employee must establish a causal link showing that their "response was in fact used thereafter as a basis for a decision affecting his or her compensation." *Farrell v. Planters Lifesavers Co.*, 206 F.3d 271, 282 (3d Cir. 2000). In considering the causal connection, the court "should not be constrained; rather, the court can consider circumstantial evidence and draw inferences in favor of the non-moving party in reaching this determination on summary judgment." *Id.* at 283.

i. Durenleau's Quid Pro Quo Sexual Harassment Claim

The substance of Durenleau's quid pro quo sexual harassment claim is joking between Tasey Leitzell, Schaar, and Sharma that Durenleau should sleep with Kusic so that he would leave them alone. NRA, Kusic, and Sharma argue Durenleau was not subject to quid pro quo sexual harassment because the sexual harassment she experienced was actually a running joke in the office and no employment benefits were attached to it. (Doc. 163, p. 111.) Durenleau argues that because she did not report this incident or others, she continued to receive

promotions. (Doc. 176, p. 41.) However, once she reported the incident where Sharma slapped her, she was "forced out of her employment." (*Id.*)

Here, there is no evidence showing a causal connection between the "joking" that Durenleau states as the basis for her claim and any later employment decisions. Even though different inferences could be drawn about the fall out from Durenleau reporting Sharma's slap, that still does not provide a connection between any rejection or submission to these "jokes" and employment decisions made by NRA. Therefore, summary judgment is granted in favor of NRA, Kusic, and Sharma on Counts II and V of Durenleau's counterclaims.

ii. Badaczewski's Quid Pro Quo Sexual Harassment Claim

Badaczewski's quid pro quo sexual harassment claim is based on the trip to buy candy for the office where Kusic bought her candy, inquired if other guys buy her as much stuff as he did, and then she was fired the next day. NRA and Kusic argue Badaczewski cannot support her quid pro quo sexual harassment claims because there is no evidence showing that any sexual advances were tied to a condition of employment. (Doc. 163, p. 135.)

Here, the evidence supporting Badaczewski's claims of Kusic making sexual advances towards her consists of statements, but Badaczewski has provided no further details regarding any specific times where these statements occurred. (Doc. 174, ¶ 829.) Additionally, Badaczewski points to the candy shopping incident

where she was fired the next day. However, on that trip, there is no evidence that Badaczewski rebuffed any advance. More specifically, there is no evidence of her response to his questions about other men buying her as many things as he does. There is also sufficient undisputed evidence to show that the decision to fire her the next day was made contemporaneously with NRA discovering that Badaczewski was the one who sent Durenleau the password spreadsheet. (Doc. 174, pp. 300–08.) Considering all of the evidence, Badaczewski cannot prove the causation element of her quid pro quo sexual harassment claim when there is clear evidence of a legitimate reason for her termination. Thus, summary judgment will be entered in favor of NRA and Kusic on Counts II and V of Badaczewski's counterclaims.

4. Retaliation Claims

To state a claim for retaliation under Title VII, a plaintiff must allege that: "(1) she engaged in activity protected by Title VII; (2) the employer took an adverse employment action against her; and (3) there was a causal connection between her participation in the protected activity and the adverse employment action." *Moore v. City of Phila.*, 461 F.3d 331, 340–41 (3d Cir. 2006) (citing *Nelson v. Upsala Coll.,* 51 F.3d 383, 386 (3d Cir.1995)).

Protected activity ranges from formal charges of discrimination to "informal protests of discriminatory employment practices, including making complaints to

management, writing critical letters to customers, protesting against discrimination by industry or society in general, and expressing support of co-workers who have filed charges." *Mufti v. Aarsand & Co., Inc.*, 667 F. Supp. 2d 535, 552 (W.D. Pa. 2009). To determine whether an employee has engaged in protected activity, "we look to the message . . . conveyed [by a plaintiff's conduct] rather than the means of conveyance. The complaint must allege that the opposition was to discrimination based on a protected category." *Daniels v. Sch. Dist. of Phila.*, 776 F.3d 181, 194 (3d Cir. 2015) (citations omitted). In undertaking the protected activity, "the employee must hold an objectively reasonable belief, in good faith, that the activity they oppose is unlawful under Title VII." *Moore*, 461 F.3d at 341.

The retaliatory action taken against the employee must be "'materially adverse' in that [it] may well have dissuaded a reasonable worker from making or supporting a charge of discrimination.'" *Id.* (quoting *Robinson*, 120 F.3d at 1300). Additionally, "a transfer to a less desirable position or an unsatisfactory job evaluation may constitute the requisite adverse employment action as to the terms, conditions, and privileges of employment, but modest changes in duties or working conditions and actions that simply make an employee unhappy but not producing a material disadvantage do not." *U.S. Equal Emp. Opportunity Comm'n v. Bob Evans Farms, LLC*, 275 F. Supp. 3d 635, 659 (W.D. Pa. 2017).

Finally, the causal connection element looks to the reason for the harassment, and "identif[ies] what harassment, if any, a reasonable jury could link to a retaliatory animus." *Id.* (quoting *Jensen v. Potter*, 435 F.3d 44, 449 n.2 (3d Cir. 2006) (*overruled in part on other grounds by Burlington N. & Santa Fe Ry. Co v. White*, 548 U.S. 53 (2006)). Temporal proximity can be used to show a causal connection if it is unusually suggestive. *Daniels*, 776 F.3d at 196. Absent unusually suggestive temporal proximity, "we consider the circumstances as a whole, including any intervening antagonism by the employer, inconsistencies in the reasons the employer gives for its adverse action, and any other evidence suggesting that the employer had a retaliatory animus when taking the adverse action." *Id.*

i. Durenleau's Retaliation Claim

Durenleau's retaliation claim includes three types of retaliatory acts. First, Durenleau alleges she was retaliated against while still working at NRA by having her parking space taken away, no longer being permitted to arrive to work early, being the only manager without a laptop, being removed from the e-team, being the subject of false fraud allegations, being forced to work while on COVID leave, and eventually having a baseless corrective action report which threatened termination on the next infraction. (Doc. 142, pp. 41–45.) Second, Durenleau alleges she was constructively discharged in retaliation for her report. (*Id.*) Third,

Durenleau alleges she was retaliated against after her employment ended by the filing of the instant lawsuit and NRA threatening discrimination charges. (*Id.*) On the other hand, NRA argues that Durenleau was not retaliated against because her report of the slap incident was not a protected activity, many of the instances of retaliation she recounts had legitimate reasons, she voluntarily resigned, and her attorney's demand letter was not a protected activity. (*Id.* at 114–30.) The court will address each type of retaliatory conduct in turn.

Turning to the conduct while Durenleau was still employed at NRA, Durenleau's emailed statement to in house counsel regarding the slap incident is protected activity because it is a complaint to management regarding Sharma's actions which could be considered sexual harassment. Durenleau does not call the incident "sexual harassment," but it is clear that she believed the slap was inappropriate and needed to be reported. Further, Durenleau made this statement in good faith and believed the slap was unlawful under Title VII because in the email she stated, "I want this on file just in case I lose my job, get demoted or have my pay reduced[,]" and she immediately reported the incident. (Doc. 162-1, p. 6.) Durenleau's actions after the slap show that she knew this incident was something out of the ordinary and that she needed to get NRA's legal counsel involved. Drawing all reasonable inferences in favor of Durenleau, a reasonable jury could

find that she was reporting an act of sexual harassment, making this email a protected activity.

Next, having her parking space taken away, not being allowed to go to work early, and being denied a work laptop, taken in totality with Daube's comment that "once you stiff him [Sharma], you're done" and the corrective action report for the allegedly fraudulent transfer of accounts wherein she was warned that her next violation would result in termination of her employment, is an adverse employment action which would dissuade a reasonable employee from filing a formal charge of discrimination. These actions, which marked a change in how she had operated at NRA, all occurred after she reported the November 2020 slap. Drawing all reasonable inferences in favor of Durenleau, a reasonable jury could find that these changes collectively rise to the level of a materially adverse employment action.

NRA provides non-discriminatory reasons for these decisions, but Durenleau alleges that these reasons are merely pretext because of the comment "once you stiff [Sharma], you're done." Further, Durenleau points to past employees who complained about the working environment of NRA and were also threatened with a lawsuit. This is sufficient to create a disputed issue of material fact regarding whether Durenleau suffered an adverse employment action.

Finally, turning to causation, Durenleau argues that all of the more minor retaliatory actions, as well as the corrective action report, coupled with Daube's comments show retaliatory animus. Daube knew that Durenleau had made a complaint about Sharma slapping her because she sat in on the investigation into the incident. (Doc. 161-16, p. 27.) After this investigation, there was a change in how NRA treated Durenleau. Some implicit facets of her employment situation, such as parking near the front and arriving at work early, were taken away. There was a corrective action report that was issued approximately two months after Durenleau reported the slap, the subject of which was allegedly fraudulent account transfers that Durenleau did not realize were against the rules. The timing of these changes is sufficient to create a dispute of material fact regarding whether they were taken with retaliatory animus. Therefore, NRA, Kusic, and Sharma's motion for summary judgment will be denied regarding Durenleau's retaliation claim while she was still employed at NRA.

Turning to Durenleau's constructive discharge claim, an employee must establish "the employer knowingly permitted conditions of discrimination in employment so intolerable that a reasonable person subject to them would resign." *Aman*, 85 F.3d at 1084. In making this determination, the court employs an "objective standard, requiring no more than a finding that the conduct complained of would have the foreseeable result that working conditions would be so

unpleasant or difficult that a reasonable person in the employee's shoes would resign." *Goss v. Exxon Off. Sys. Co.*, 747 F.2d 885, 887–88 (3d Cir. 1984). The court must consider, "whether the employee was threatened with discharge, encouraged to resign, demoted, subject to reduced pay or benefits, involuntarily transferred to a less desirable position, subject to altered job responsibilities, or given unsatisfactory job evaluations." *Colwell v. Rite Aid Corp.*, 602 F.3d 495, 503 (3d Cir. 2010). Further, "[a] hostile work environment 'will not always support a finding of constructive discharge.'" *Spencer v. Wal-Mart Stores, Inc.*, 469 F.3d 311, 317 (3d Cir. 2006) (quoting *Marrero v. Goya of P.R., Inc.*, 304 F.3d 7, 28 (1st Cir. 2002)). There must be a greater showing of severity or pervasiveness than in a hostile work environment claim. *Id.*

Here, Durenleau was threatened with discharge through the corrective action report that provided her next violation would result in termination. Durenleau has also provided sufficient facts to create a dispute regarding whether she suffered a hostile work environment, as previously discussed. Additionally, as discussed above, she also showed a crackdown on her behavior after reporting the slap incident with Sharma. Similar to *Aman v. Cort Furniture Rental Corp.*, 85 F.3d 1074, 1084 (3d Cir. 1996), Durenleau has established that she faced a pattern of discrimination for several years and then faced an uptick in negative consequences after she reported the clap incident. A reasonable employee could feel compelled

to quit when confronting these circumstances. Accordingly, NRA, Sharma, and Kusic's motion for summary judgment on Durenleau's constructive discharge retaliation claim is denied.

Finally, turning to Durenleau's retaliation claims post-resignation, "a plaintiff must show that [s]he engaged in protected activity, that [her] former employer had influence over a subsequent employment-related decision, and that [her] former employer made a retaliatory use of that influence to the detriment of the plaintiff's employment opportunities." *Boandl v. Geithner*, 752 F. Supp. 2d 540, 567 (E.D. Pa. 2010) (citing *Charlton v. Paramus Bd. of Educ.*, 25 F.3d 194, 200–201 (3d Cir. 1994)).

NRA argues that her criminal complaint and her attorney's notice of claims was not a protected activity because it did not refer to the slap incident as "sexual harassment." (Doc. 163, p. 126–27.) However, as we held above regarding Durenleau's email, the notice references the slap incident, which could be sexual harassment, as it is unlikely that Sharma would slap a male employee. Next, Durenleau provides evidence that Kusic emailed her supervisor at her new job, pointing them towards evidence in this case showing that Durenleau had her boyfriend, a police officer, check for information on this individual. (Doc. 173-2, p. 2.) This email was sent the day after she was terminated by her subsequent employer. (Doc. 161-8, p. 19.) There is no other evidence in the record regarding

why she was terminated from her subsequent position besides Durenleau's speculation that someone contacted her new employer prior to her termination. Durenleau's speculation is not sufficient to establish a causal connection. Therefore, summary judgment is granted in favor of NRA, Kusic, and Sharma on Durenleau's post-resignation retaliation claim.

In conclusion, NRA, Kusic, and Sharma's motion for summary judgment is granted regarding Durenleau's post-resignation retaliation claim but denied regarding Durenleau's retaliation claim while at NRA and her constructive discharge claim.

ii. Badaczewski's Retaliation Claim

NRA argues that Badaczewski can provide no evidence of a causal connection for her retaliation claim where she was terminated for legitimate business reasons. (Doc. 163, p. 137.) Badaczewski argues that her termination occurred after Badaczewski made a report to HR regarding Kusic's intimidating conduct with her. (Doc. 173, p. 53.)

Here, Badaczewski's email to HR consisted of complaints that Kusic made "rude condescending comments towards me about my intelligence, work ethic, and ability to grasp something." (Doc. 161-13, p. 24.) This email is entirely regarding her ability to perform her job and makes no reference to any comments that could be related to her sex in anyway. However, in a subsequent meeting with HR

regarding the email, she told the HR director and Lisa Daube about Kusic "constantly talk[ing] about me being blond and having big boobs." (Doc. 174, ¶ 866.) These complaints are sufficiently relating to her sex that reporting them in the meeting consists of a protected activity. However, the act of terminating her is not sufficiently causally connected to these reports to constitute retaliatory animus. Initially, she sent the email and had the meeting in January and she was not terminated until March. Further, her termination is temporally very close to NRA discovering that she had been the one who logged into Durenleau's computer and sent her the spreadsheet. Therefore, Badaczewski cannot prove she was retaliated against for her complaints to HR about Kusic's potential sexual harassment. Summary judgment will be granted in favor of NRA and Kusic on Counts III and VI of Badaczewski's counterclaims.

5. PHRA Claims against Kusic and Sharma Individually

i. Durenleau's Individual Claims

Kusic and Sharma argue that Durenleau's individual claims against them fail because they are untimely, and she fails to show a PHRA violation. (Doc. 163, p. 130.) First, Durenleau's claims are timely because the continuing violation doctrine applies to PHRA claims as well as Title VII claims. *Lesko v. Clark Publisher Svcs.*, 904 F. Supp. 415, 419 (M.D. Pa. 1995). Here, Durenleau filed her EEOC and PHRA charge within 180 days after the November 20, 2020, slap.

(Doc. 161-23.) Since the court held that the continuing violation doctrine applies to the Title VII claim, it applies to the individual PHRA claims for the same reasons.

Second, the PHRA establishes liability for employers for unlawful employment practices, but also provides that it is unlawful for "any person, employer, employment agency, labor organization or employe[e], to aid, abet, incite, compel or coerce the doing of any act declared by this section to be an unlawful discriminatory practice . . . ." 43 PA. STAT. § 955(a), (e). Further, "in the appropriate factual scenario, an individual supervisory employee can be held liable under an aiding and abetting/accomplice liability theory . . . for his own direct acts of discrimination or for his failure to take action to prevent further discrimination by an employee under supervision." *Davis v. Levy, Angstreich, Finney, Baldante, Rubenstein & Coren P.C.*, 20 F. Supp. 2d 885, 887 (E.D. Pa. 1998) (citing *Dici v. Commonwealth of Pa.*, 91 F.3d 542, 552 (3d Cir. 1996)). The appropriate circumstances to find a supervisor liable for his own discrimination is when they "engage[] in discriminatory conduct while acting in the scope of his employment" because they "share[] the intent and purpose of the employer and may [properly] be held liable for aiding and abetting the employer in its unlawful conduct." *Glickstein v. Neshaminy Sch. Dist.*, No. 96–6236, 1997 WL 660636, at *12 (E.D. Pa. Oct. 22, 1997).

Here, the aiding and abetting count against Sharma can proceed because Sharma was Durenleau's supervisor at the time of the alleged harassment and the harassment occurred while at work, in the scope of their supervisor-direct report relationship. Further, the individual liability claim can go forward against Kusic because he is the CEO of NRA and can be said to "share the intent and purpose" of the employer. Accordingly, NRA, Kusic, and Sharma's motion for summary judgment will be denied as to Count IV of Durenleau's counterclaims.

ii. Badaczewski's individual claims

Kusic argues Badaczewski's individual claims against Kusic fail because she fails to show a PHRA violation. (*Id.* at 144.) For the same reasons that Durenleau's claims against her supervisor will go forward, so will Badaczewski's. Kusic's motion for summary judgment will be denied as to Count IV of Badaczewski's counterclaims.

CONCLUSION

Durenleau and Badaczewski's motion for summary judgment regarding NRA's claims against them is granted. NRA, Kusic, and Sharma's motion for summary judgment on Durenleau and Badaczewski's counterclaims will be granted in part and denied in part. An order follows.

s/Jennifer P. Wilson
JENNIFER P. WILSON
United States District Judge
Middle District of Pennsylvania

Dated: December 19, 2023

CERTIFICATE OF SERVICE

I, Paige Macdonald-Matthes, certify that on December 18, 2025, I served counsel of record with a true and correct copy of NRA Group, LLC's *Application to Recall and Stay Mandate* via U.S. First Class Mail and email:

Cory A. Iannacone, Esquire
Pillar Aught
4201 E. Park Circle
Harrisburg, PA 17111
ciannacone@pillaraught.com

Paige Macdonald-Matthes, Esquire
Paige Macdonald-Matthes, Esquire