PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 23-3017

UNITED STATES OF AMERICA

v.

FRANCES M. EDDINGS, a/k/a Fran Eddings,

Appellant

Appeal from the United States District Court
for the Eastern District of Pennsylvania
(District Court No. 5:19-cr-00535-001)
District Judge: Honorable Joseph F. Leeson, Jr.

Argued September 17, 2025

Before: BIBAS, MONTGOMERY-REEVES, and AMBRO,
Circuit Judges

(Opinion filed: December 9, 2025)

Benjamin B. Cooper **(Argued)**
Daigle Cooper & Associates
535 W Hamilton Street
Suite 105
Allentown, PA 18101

Counsel for Appellant

Paul G. Shapiro **(Argued)**
Robert A. Zauzmer
Office of United States Attorney
615 Chestnut Street
Suite 1250
Philadelphia, PA 19106

Counsel for Appellee

OPINION OF THE COURT

AMBRO, *Circuit Judge*

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, prohibits accessing a computer "without authorization." Recently, we considered when an employee is authorized to access her employer's computer. We answered: when her employer gives her permission to use it. *NRA Grp., LLC v. Durenleau*, 154 F.4th 153, 168 (3d Cir. 2025). Today, we consider when an employee is no longer authorized to access her employer's computer. We answer: when her employer rescinds her permission to use it. In this case, the employee resigned from her job, then accessed her employer's email account. But her employer had not taken a single step to rescind her permission to use it. And no contract linked the employer's authorization to her employment. For that reason, we vacate the conviction of Frances Eddings as an accomplice and co-conspirator to accessing the employer's computer "without authorization."

I. BACKGROUND

On August 14, 2014, Jude Denis started a job helping the Prostate Cancer Foundation (PCF) organize a fundraiser. To plan the event, Denis needed to read, write, and send emails on behalf of a PCF board member, Neil Rodin, so PCF installed a link on Denis's personal computer that would enable her to use Rodin's account without knowing the password herself.

After a few days, her relationship with PCF deteriorated. She thought it had hired her for a permanent, full-time position. PCF thought she had accepted a temporary role as a contractor in the hope of future consideration for a promotion. On August 21, Denis declined to continue her work, emailing Rodin and a colleague, "Thanks again for your kind offer, but I can't possibly accept it." SAppx1124. She asked for payment for the days she worked and reimbursement for her expenses, submitting an invoice for a few thousand dollars for "my time at PCF." SAppx1126.

PCF did not pay. In fact, it ceased communicating with Denis. To negotiate payment, she enlisted the help of a friend, Appellant Frances Eddings. They devised a plan. Denis still had access to Rodin's email account. Beginning September 22, she read his emails, downloaded internal PCF documents, and sent them to Eddings. Eventually, Eddings emailed PCF's CEO with a threat to release thousands of the PCF documents if the organization did not satisfy Denis's demand for lost wages—now $150,000—and Eddings's own demand for a 25% fee. Instead, on October 1 PCF remotely disabled the link on Denis's computer—ending her access to Rodin's account—and reported Denis and Eddings to the FBI.

In September 2019, a grand jury indicted the two on four counts of violating the CFAA, 18 U.S.C. § 1030, which in relevant part prohibits intentionally accessing another's computer "without authorization." Eddings was indicted as Denis's co-conspirator and accomplice.

Their joint trial in April 2022 proceeded on the prosecution's theory that Denis resigned on August 21, 2014, and that her resignation ended her authorization to access Rodin's account, whereupon her subsequent access was "without authorization." After the Government presented its case-in-chief, Eddings moved under Federal Rule of Criminal Procedure 29 for a judgment of acquittal, contending the failure to prove Denis accessed Rodin's account without authorization because PCF did not lock her out of the account until October 1. The District Court denied the motion.

At closing argument, Eddings's counsel tried to discredit the prosecution by arguing the Government had charged Eddings with violating the CFAA in a desperate bid to pin her with something after failing to find enough evidence to charge her with extortion. The Government exercised its right to offer a rebuttal. Its counsel explained the role of extortion in the case:

> No one's sitting here arguing that the defendants are charged with extortion. They're not. They're charged with – because it was unsuccessful. They didn't get the money. The reason the money in this case is important is, it's because of the reason for the computer intrusion. And, then that's part of what you need to find.

SAppx1115. When the prosecutor concluded his rebuttal, Eddings moved for a mistrial, taking issue with the Government's insinuation that it would have charged her with extortion if she had procured any money. The District Court denied the motion. However, it gave a curative instruction:

> Extortion is not, repeat, not a part of this case. The defendants are not charged with extortion. You are not to consider that subject in your jury deliberations. Why a charge of extortion was not brought is not relevant and not to be considered . . . and any argument[] by any of the lawyers or any of the parties in this case about that subject is to be disregarded by you.

SAppx1002.

To define the phrase "without authorization," the District Court gave the jury an instruction Eddings requested, followed by two additional sentences of its own devising:

> A person uses a computer without authorization when the person has not received permission from the person who controls the

> right of access to the computer for any purpose,
>
> or
>
> when the person who controls the right of access to the computer has withdrawn or rescinded permission to use the computer and the person uses the computer anyway.
>
> *Once given, a person's authorized access may be revoked. Whether authorized access has been revoked or, whether the cessation of employment rescinds authorization, is a factual question for you to decide as the jury*.

Appx027 (additions to Eddings's requested instruction in italics).

The jury found Denis and Eddings guilty on all counts. Denis died shortly afterward. Eddings's sentence was 18 months' probation, six of which she served on home confinement.

Eddings moved under Rule 33 for a new trial on several grounds, including that the jury instruction on authorization misstated the law and that the prosecutor's closing remarks about extortion were inappropriate. The District Court denied the motion.

Eddings appeals, challenging the denial of her Rule 29 motion for judgment of acquittal and the denial of her Rule 33 motion for a new trial on the basis of the jury instruction and the prosecutor's remarks about extortion.

II. JURISDICTION AND STANDARDS OF REVIEW

The District Court had jurisdiction under 18 U.S.C. § 3231. We have jurisdiction over the final judgment and post-trial orders under 28 U.S.C. § 1291.

Our review of a district court's denial of a Rule 29 motion for judgment of acquittal is plenary. *United States v. John-Baptiste*, 747 F.3d 186, 201 (3d Cir. 2014) (citation omitted). We review the sufficiency of the evidence under a "highly deferential" standard, overturning the jury's verdict only if, viewing the evidence in the light most favorable to the prosecution, "no reasonable juror could accept the evidence as sufficient to support the conclusion of the defendant's guilt beyond a reasonable doubt." *United States v. Caraballo-Rodriguez*, 726 F.3d 418, 430–31 (3d Cir. 2013) (*en banc*) (quotation omitted).

We review for abuse of discretion a district court's denial of a motion for a new trial. *United States v. Silveus*, 542 F.3d 993, 1005 (3d Cir. 2008). How we review jury instructions depends on how they are challenged. Where "the question is whether the jury instructions stated the proper legal standard, our review is plenary." *O'Brien v. Middle E. F.*, 57 F.4th 110, 117 (3d Cir. 2023) (quoting *United States v. Coyle*, 63 F.3d 1239, 1245 (3d Cir. 1995)). If the instruction incorrectly stated the law, "a new trial is required unless there is a high probability that [it] did not affect the outcome of the case." *Id.* at 121 (cleaned up). However, where the question is whether the instruction expressed the legal standard with sufficient clarity, we review for abuse of discretion. *United States v. Zehrbach*, 47 F.3d 1252, 1264 (3d Cir. 1995) (*en banc*). We consider "whether, viewed in light of the evidence, the charge as a whole fairly and adequately submits the issues in the case to the jury." *Id.* (quoting *Bennis v. Gable*, 823 F.2d 723, 727 (3d Cir. 1987)). "We must reverse if the instruction was capable of confusing and thereby misleading the jury." *United States v. Shaw*, 891 F.3d 441, 450 (3d Cir. 2018) (cleaned up).

III. DISCUSSION

The jury convicted Eddings of four counts of violating the CFAA: three counts of accessing a computer in violation of 18 U.S.C. § 1030(a)(2), and one count of conspiracy in violation of 18 U.S.C. § 1030(b). So we start with her CFAA arguments. We then discuss her argument regarding the prosecutor's closing remarks about extortion.

A. The District Court erred in denying Eddings's Rule 29 motion for judgment of acquittal.

To prove Eddings violated the CFAA with Denis, the Government had to prove the latter "(1) intentionally (2) accessed without authorization . . . a (3) protected computer and (4) thereby obtained information." *United States v. Auernheimer*, 748 F.3d 525, 533 (3d Cir. 2014) (citation omitted). Virtually every computer is a "protected computer" because the phrase covers any computer "used in or affecting interstate or foreign commerce or communication," *NRA*, 154 F.4th at 165 (quoting 18 U.S.C. § 1030(e)(2)(B)), which encompasses at least "all computers that connect to the Internet," *Van Buren v. United States*, 593 U.S. 374, 379 (2021).

Eddings's appeal concerns only the second element, authorization. The parties have stipulated that PCF authorized

Denis to access Rodin's account when she began her role there on August 14, 2014. The Government claimed Denis resigned on August 21 and subsequently accessed Rodin's account until PCF terminated her access on October 1. Was that evidence, construed in the Government's favor, sufficient for a rational jury to find Denis accessed Rodin's account when she was no longer authorized to do so?

Before we assess the sufficiency of the evidence, we must consider what it must be sufficient to prove. Eddings contends that for Denis to access Rodin's account without authorization, the Government had to prove PCF revoked her access first and she then hacked her way in. If Eddings is right about the law, then the evidence was insufficient to sustain her conviction: there is no dispute PCF did not lock Denis out of the account until October 1, and she did not access the account again.

The Government asserts that to prove Denis accessed the account without authorization, it only had to show she resigned and accessed the account afterward. If that is the law, then the evidence was sufficient to sustain the verdict, at least under the highly deferential standard that controls our review. Although Eddings insists Denis merely paused her work to negotiate better terms, a reasonable jury could have found she resigned on August 21.

Framing the issue are two significant facts. First, the record contains no evidence that PCF conditioned Denis's permission to access Rodin's account on her continued employment. True, Denis signed a confidentiality agreement governing her "access to certain [c]onfidential [i]nformation" while at PCF. SAppx1121. But that agreement did not impose any restrictions on Denis's access, let alone specify that her access would end if she resigned. Second, the record contains no evidence Denis's employer took any affirmative step to rescind her permission to use the account after she resigned—until, of course, by revoking her access on October 1.

In this distinctive context, we believe the statute charts a middle way. To prove Denis accessed the account without authorization, the Government had to prove PCF revoked her authorization to do so. At least in the absence of any contract linking authorization with employment, this required proving PCF took some step to withdraw the permission it gave her. Proving she resigned was not enough.

1. Denis accessed Rodin's account "without authorization" if, but only if, she accessed it after PCF revoked her permission to use it.

Whether an employee is authorized to access her employer's computer is up to her employer. Only it has the power to grant her authorization. And only it has the power to rescind that authorization. PCF no doubt gave Denis permission to access Rodin's email. So it had to rescind its permission for Denis's access to be unauthorized.

a. In the absence of a contract saying so, an employee's resignation alone does not rescind her employer's authorization for her to use her employer's computer.

Section 1030(a)(2) of the CFAA proscribes "intentionally access[ing] a computer without authorization." 18 U.S.C. § 1030(a)(2). The "without authorization" phrase "protects computers themselves by targeting so-called outside hackers—those who 'acces[s] a computer without any permission at all.'" *Van Buren*, 593 U.S. at 389 (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)).

The statute does not define "authorization." We have. In *NRA* we held "an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer." *NRA*, 154 F.4th at 168 (quoting *Teva Pharms. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 670 (E.D. Pa. 2018)). That is because authorization is "permission or power granted by an authority." *United States v. Nosal*, 844 F.3d 1024, 1035 (9th Cir. 2016) (quoting *Brekka*, 581 F.3d at 1133). *See also Abu v. Dickson*, 107 F.4th 508, 516 (6th Cir. 2024). In the employment context, the authority is the employer. *See Brekka*, 581 F.3d at 1135; *Abu*, 107 F.4th at 516 (describing authorization as a function of "a company's sanction or permission"). One way an employee accesses a computer "without authorization," then, is by accessing the computer without her employer granting permission.

Just as authorization can be given, it can be taken away. *Nosal*, 844 F.3d at 1035 ("Implicit in the definition of authorization is the notion that someone, including an entity, can grant or revoke that permission."). By whom? In the employment context, it is again the employer. *See id.* at 1035–36; *Abu*, 107 F.4th at 516. Once it has authorized an employee to access its computer, only it has the power to revoke the authorization it granted. Hence a second way an employee accesses a computer "without authorization" is "when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Brekka*, 581 F.3d at 1135.

Absent more, an employee's resignation does not cancel her employer's authorization. The reason: an employee's resignation is not her employer's action. It is her own. An employee cannot rescind the permission her employer gave her any more than an employee can provide permission her employer has not given. Only her employer can do that. After all, whether an employee is authorized to access her employer's computer "depends on actions taken by the employer." *Id.* Thus, absent prior agreement, an employee's resignation does not revoke her employer's authorization. Her employer must perform some affirmative act to revoke it.[1] *Accord Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] defendant can run afoul of the

[1] Our interpretation aligns with the theory that the CFAA's ban on access "without authorization" embeds "trespass norms—broadly shared attitudes about what conduct amounts to an uninvited entry into another person's private space." *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1146 (2016). On this theory, permission to use an account is a delegation of the right to access the account. *Id.* at 1175. "[T]he owner's revocation of the right to use an authenticated account revokes authorization. When the computer owner communicates the revocation to the user, the delegated authority ends." *Id.* After that, "[s]ubsequent account access violates trespass norms." *Id.*

CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly.").

Context reinforces the text. Recall the CFAA bars "intentionally access[ing] a computer without authorization." 18 U.S.C. § 1030(a)(2). We have suggested "that 'intentionally' modifies the entire" provision. *See NRA*, 154 F.4th at 168 n.7. Unless and until the employer affirmatively rescinds the permission it gave an employee, that employee may not know her employer's sanction has ended, and hence may not have the state of mind required to violate the statute. *See Abu*, 107 F.4th at 517.

Precedent confirms that an employee's authorization ends only when the employer ends it. The sole circuit to weigh in precedentially has suggested an employer must take some action of its own to revoke an employee's authorization.[2] No

[2] The Sixth Circuit suggested a similar interpretation in *United States v. Shahulhameed*, 629 F. App'x 685 (6th Cir. 2015), a nonprecedential opinion later cited approvingly in a precedential one, *Abu*, 107 F.4th at 516. After an IT contractor for Toyota fired Ibrahimshah Shahulhameed from the firm, he used his work account to launch a cyberattack on Toyota's systems. 629 F. App'x at 687–88. The Court held his former employer had revoked his access before the attack by firing him, informing him his project had been terminated, and ordering him not to communicate with his former colleagues or report to Toyota again. *Id.* at 688. The Sixth Circuit subsequently has posited *Shahulhameed* as "concluding that firing an employee cut off his 'authorization' to access company accounts." *Abu*, 107 F.4th at 516. Again, what ends

circuit has endorsed the Government's view that an employee's resignation alone revokes the permission her employer gave her to access company computers in the absence of a contract saying so.

In *Nosal*, the Ninth Circuit concluded that three employees lost the authorization to access their employer's systems when the employer revoked their credentials, rather than when (and because) they resigned. *Nosal*, 844 F.3d at 1029, 1034, 1036. The three employees had downloaded proprietary information from the employer's system in preparing to quit and start a competing firm. *Id.* at 1031. Two of them then left the company entirely and the third resigned his full-time role but stayed on as a contractor. *Id.* The company soon thereafter revoked their credentials—locking them out of the system. *Id.* In response, they convinced a colleague who had stayed at the company to let them use her credentials so they could continue logging in. *Id.*

The Ninth Circuit affirmed their convictions for violating the CFAA by using their colleague's credentials after the company terminated theirs. *Id.* at 1028–30. Employees lose the authorization to access their employer's systems "when [it] has rescinded permission to access the computer." *Id.* at 1029 (quoting *Brekka*, 581 F.3d at 1135). And the defendants' employer rescinded the permission it gave them when the company revoked their credentials shortly after they resigned. *See, e.g.*, *id.* at 1036 ("Korn/Ferry also rescinded Christian and Jacobson's credentials after they left, *at which point* the three

an employee's authorization is his employer's conduct—there, the affirmative act of firing him.

former employees were no longer 'insiders' . . . [but r]ather had become 'outsiders' with no authorization to access Korn/Ferry's computer system.") (emphasis added); *id.* at 1038 (holding "a former employee whose computer access credentials were affirmatively revoked by [his employer] acted 'without authorization' in violation of the CFAA"). Thus we repeat: an employee's authorization to use his employer's computer ends when his employer takes an affirmative step to revoke it, not simply when he resigns.

The Government contends the Ninth Circuit's decision in *Brekka* says an employee's resignation alone rescinds his employer's authorization. Our dissenting colleague shares the Government's take. *Brekka* affirmed a district court's grant of summary judgment for the defendant employee, Christopher Brekka, in a civil CFAA case. 581 F.3d at 1129. The Government claims a passage at the start of the second portion of the opinion concludes resignation is revocation: "There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company[,] . . . [he] would have accessed a protected computer 'without authorization' for purposes of the CFAA." *Id.* at 1136. We reject the Government's interpretation of this sentence, and respectfully part ways with our colleague, for four reasons.

First, in that procedural posture—an appeal from a grant of summary judgment—this sentence appears to be a statement of the parties' views. All three other times *Brekka* uses the phrase "no dispute," it does so in the sense distinctive to summary judgment, that is, to refer to the matters the parties do not disagree about. *See id.* at 1133 ("there is no dispute that Brekka had permission to access the computer"), *id.* ("there is no dispute that Brekka was still employed by LVRC when he emailed the documents to himself"), *id.* at 1135 ("There is no dispute that Brekka was given permission to use LVRC's computer . . ."). Thus there is no reason to think here the Ninth Circuit used the phrase to signal it was adopting a novel legal position without any explanation.

Second, *Brekka*'s own formulation of its holding provides that once an employer has permitted an employee's access, his access becomes unauthorized only once the employer takes back permission: "[W]e hold that a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or *when the employer has rescinded permission* to access the computer and the defendant uses the computer anyway." *Brekka*, 581 F.3d at 1135 (emphasis added). If that were not clear enough, the Court underscored that, under "the plain language of the statute . . . [, authorization to use an employer's computer] depends on actions taken by the employer," *id.* (quotation omitted), and an employee's resignation is hardly an "action[] taken by the employer." *See id.*

Third, Brekka did not just walk away from LVRC. Although the record is murky, it appears, after contract negotiations broke down, LVRC either fired Brekka or he and the company agreed to part ways. *See LVRC Holdings, LLC v. Brekka*, No. 2:05-CV-01026-KJD-GWF, 2007 WL 2891565, at *1, *4 (D. Nev. Sept. 28, 2007). *See also Nosal*, 844 F.3d at 1034 ("LVRC terminated his employment."). Either way, what was at issue was an employer's conduct as well—not just an employee's unilateral resignation.

Fourth, the Government's reading is inconsistent with how the Ninth Circuit has read *Brekka* since. In *Facebook*, the Court "distill[ed]" from *Brekka* that "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly." *Facebook*, 844 F.3d at 1067. And as discussed above, in *Nosal* it held three employees accessed their employer's system without authorization not once they resigned, but once their employer revoked their access shortly thereafter. *Nosal*, 844 F.3d at 1034, 1036, 1038. It took itself to be "reiterat[ing]" *Brekka*'s holding that authorization expires "when the employer has rescinded permission." *Id.* at 1029. If the Government is right that *Brekka* held resignation suffices for revocation, then *Nosal* was not reiterating *Brekka* but revising it.[3]

The assumption that resignation ends authorization might seem like "common sense." *See Steele*, 595 F. App'x at

[3] The Government also cites the Fourth Circuit's nonprecedential opinion in *United States v. Steele*, 595 F. App'x 208 (4th Cir. 2014). If anything, it favors our interpretation. Steele was a business executive and technology administrator who logged into his former employer's systems for months after he resigned. *Id.* at 209. The Fourth Circuit affirmed his CFAA conviction, holding he lacked authorization for this post-resignation access. *Id.* At first, the Court noted "the fact that Steele no longer worked for SRA when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer

211. Reality is more complicated. After an employee resigns, he might continue on for a while as a contractor without any change in his privileges. *See Nosal,* 844 F.3d at 1029. If he was working from home, he might use his work email account on his work laptop to ask his former manager when he should return the equipment. *See Clarity Servs., Inc. v. Barney,* 698 F. Supp. 2d 1309, 1311–12 (M.D. Fla. 2010). Or he might email a supplier to help his busy boss wind down some ongoing business. *See id.* Sometimes, an employer will be fine with this continued access. (Perhaps the employer is preparing to offer the employee a raise to stay or return.) Other times, an employer will insist that with the end of employment comes the end of authorization. *See id.* at 1312. But that is the point. Whether an employee's resignation spells the end of his permission to access the employer's computer is up to the computer's owner, the employer.

The policy implications of the Government's position—this sort of conduct may be criminal the moment an employee resigns simply because he resigns—are almost as "breathtaking" as those that encouraged the Supreme Court to read the statute narrowly in *Van Buren* and us to read the CFAA narrowly in *NRA*. *See Van Buren*, 593 U.S. at 393; *NRA*, 154 F.4th at 167. When Congress prohibited employees from

existed." *Id.* at 211. But counter to the Government's interpretation, the Court did not rest its holding on this mere suggestion. Instead, it held "the evidence provides ample support for the jury's verdict" because "SRA took steps to revoke Steele's access to company information, including collecting Steele's company-issued laptop, denying him physical access to the company's offices, and generally terminating his main system access." *Id.*

accessing their employers' computers without their employers' authorizations, Congress did not usurp employers' discretion to decide when their own permission starts and ends.

We think these considerations of text, context, precedent, and policy clarify what it means to access a computer "without authorization."[4] But if there were any ambiguity left to dispel, the rule of lenity would favor the same interpretation. This "canon of strict construction of criminal statutes" counsels us to "resolv[e] ambiguity in a criminal statute [so] as to apply it only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997). In any event,

[4] If we were inclined to consider the legislative history, we would not find much help. The House Report suggests that the Justice Department supported the enactment of the bill in part to enable the prosecution of former employees for accessing their former employers' computer systems without authorization. *See* H.R. Rep. No. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3698, 3691–92. And it mentions two such cases as examples of the sort of conduct the Department hoped the statute would permit it to prosecute. *See id.* Assume those cases involved resignations. (The Report does not say.) We see no reason to assume they resembled the fact pattern in front of us: an employee's unilateral resignation, without so much as a response from the employer, in the absence of any contract limiting authorization to employment. As a result, we cannot draw any conclusions from the legislative history about whether Congress contemplated a case like this, much less what Congress thought about one. For that, we have turned where the Supreme Court has directed us in interpreting the CFAA: to the text, statutory context, policy, and precedent. *See Van Buren*, 593 U.S. at 381–96.

accessing an employer’s computer after resigning but before the employer has said or done anything to rescind its permission is not “conduct clearly covered” by the CFAA. *See id.*

Our holding is narrow. First, we do not decide whether an employer revokes an employee’s authorization by firing her. Whereas resignation is the act of the employee, termination is the act of the employer. Second, we do not rule out that an employer may provide by contract that resignation terminates authorization. *Cf. Van Buren*, 593 U.S. at 390 n.8 (declining to rule out contractual restrictions on access). We have no occasion to decide that because there is no such contract in the record. Nor do we need to consider whether an employer manual noticed adequately to its employees might suffice as, once again, none exists in this record. Authorization might be a function of employment, but only so long as the employer makes it so. Third, we do not prescribe how an employer must act to revoke authorization. It might take nothing more than an email notifying the employee she is not entitled to access the system anymore. We hold only that, absent an applicable contract or policy, the employer must act. So long as there is evidence the employer took some step to rescind the employee’s permission, it is up to the jury to decide whether, as a matter of fact, that action sufficed. Fourth, as we explain next, we reject the view that the only way for an employer to revoke authorization is to revoke access.

b. An employer need not revoke an employee's access to revoke an employee's authorization.

On Eddings's account, an employer may revoke an employee's authorization to access its computer only by revoking the employee's access to the computer—that is, cutting off the employee's technical capacity to enter the system. We disagree.

Under the CFAA, "access" and "authorization" are distinct. "In the computing context, 'access' references the act of entering a computer 'system itself' or a particular 'part of a computer system,' such as files, folders, or databases." *Van Buren*, 593 U.S. at 388. "Authorization" is permission to access. *See NRA*, 154 F.4th at 168. The CFAA permits access within the scope of that authorization. *See Van Buren*, 593 U.S. at 388–89.

Access is neither necessary nor sufficient for authorization. One can obtain access without authorization: archetypally, hacking procures access by circumventing a code-based barrier like a log-in requirement. *See id.* at 389. And one can have authorization without access: if your employer requires you to update your work password every six months to log in and you let your password lapse, you might retain authorization but temporarily lose access. *See Nosal*, 844 F.3d at 1034 n.4. By asking us to hold an employer must terminate access to rescind authorization, Eddings seeks to treat access as sufficient for authorization—collapsing the distinction the statute constructs and imposing a burden on employers with no basis in the statute.

Eddings's interpretation also sits uneasily with other components of the statutory scheme. For instance, the CFAA prohibits password trafficking: illicitly trading the credentials necessary to obtain technical access to a computer without the owner's permission. 18 U.S.C. § 1030(a)(6). If access sufficed for authorization, prohibiting password trafficking would make little sense. In a similar spirit, other circuits have held defendants violated the CFAA by obtaining access to computers by misrepresenting themselves as authorized users. *See United States v. Cuomo*, 125 F.4th 354, 360–61 (2d Cir. 2025); *United States v. Phillips*, 477 F.3d 215, 218 (5th Cir. 2007).

In any event, there is no authority for the proposition that revoking authorization requires revoking access. True enough, some cases have held employers withdrew authorization by cutting off access. *See Nosal*, 844 F.3d at 1034, 1036; *Clarity Servs.*, 698 F. Supp. 2d at 1316. But revoking access in those cases was *sufficient* to revoke authorization without any indication it was *necessary* to revoke authorization. *See Nosal*, 844 F.3d at 1034 (holding former employees accessed system "without authorization" because their former employer "rescinded permission to access its computer system" by revoking their credentials); *Clarity Servs.*, 698 F. Supp. 2d at 1316 ("Clarity presents no evidence that Barney lacked authorization to read the email" until the company suspended his account). Even the cases Eddings cites for her position recognize what matters is when the employer withdraws authorization, not access. *See, e.g.*, *QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595 (E.D. Pa. 2016)

("[T]hose 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.").[5]

Authorization is permission to access a computer, not access alone. Revoking access is not necessary for revoking authorization. That Denis retained access to another's account

[5] To understand the stakes, return to *Shahulhameed*, the Sixth Circuit case of the IT contractor who used his credentials to launch a cyberattack on his former client, Toyota, after his firm fired him. 629 F. App'x at 688. What preceded Shahulhameed's firing was a credible allegation he had tried to extort a colleague. *Id.* Once his manager heard what he had done, the manager called him that very evening to fire him. *Id.* To dispel any doubt about his status, the manager followed up by email "around midnight" to convey the same message: Shahulhameed was fired, he was not to report to work again, and he was not to communicate with his colleagues anymore. *Id.* However, "[g]iven the late hour . . .[,] Toyota waited until the next business day to disable his account." *Id.* Shahulhameed insisted his employer had not withdrawn his authorization to use his account until disabling it the next day. *Id.* The Sixth Circuit rejected that view out of hand. *See id.*; *see also Abu*, 107 F.4th at 516 (observing "firing [Shahulhameed] cut off his 'authorization' to access company accounts, even though the employee could still log in"). Shahulhameed's employer affirmatively withdrew its authorization the only way it could at the time: by its spoken and written words. Nothing in the CFAA permits, let alone requires, us to make employers jump over the hurdles Shahulhameed demanded and Eddings demands here.

does not mean she retained authorization to access it. PCF had to take some step to withdraw the permission it gave her. But it did not have to lock her out.

2. No reasonable juror could have found PCF revoked Denis's authorization to access Rodin's email account after she concluded her work.

To find Denis accessed Rodin's email account without authorization, the jury needed evidence PCF took some step to rescind her permission to use the account after she resigned. The Government submitted no such evidence. Instead, it focused exclusively on proving Denis's access was unauthorized because she resigned beforehand. Tellingly, in its briefing the Government did not even attempt to point to other evidence that could enable a rational jury to find PCF withdrew Denis's authorization to use the account. Denis's resigning was the only evidence the jury had to justify a finding PCF revoked Denis's authorization. That is insufficient.

At oral argument, the Government told us a single piece of evidence could close the gap: text messages between Denis and Eddings in which Denis shared she deleted the link because she "didn't want to be tempted." *See* SAppx709–11. As the Government reads the texts, they reveal Denis knew she had been doing something wrong. The suggestion is that a jury could infer PCF took some step to rescind her authorization to use the account. The text messages may indicate a guilty conscience. Even if so, they do not say anything to suggest Denis was aware of, let alone reacting to, some unspecified affirmative step PCF took to rescind her permission to access the account. The crucial links are speculative. The jury would have had to infer Denis was feeling legal guilt, not (just) moral guilt. Then the jury would have had to infer she felt that guilt because she knew she was no longer authorized to access Rodin's account—rather than, say, because she was trying to extort a charity. And then the jury would have had to infer that what led her to think so was something PCF did, otherwise absent from the record, to withdraw permission. A criminal conviction cannot stand on so much speculation.

As a matter of law, the jury could find Denis accessed Rodin's emails without authorization only if there were evidence PCF affirmatively rescinded her permission to use the account. There was no evidence it did. For these reasons, the District Court should not have denied Eddings's Rule 29 motion for judgment of acquittal.

B. The District Court erred in instructing the jury "whether the cessation of employment rescinds authorization . . . is a factual question for you to decide."

Once an employer authorizes its employee to access its computer, the employee does so without authorization only if her employer rescinds its authorization and the employee accesses the computer anyway. The District Court, however, instructed the jury here that "whether the cessation of employment rescinds authorization, is a factual question for you to decide." SAppx1030–31. Not necessarily. An employee's resignation alone does not revoke her employer's authorization.

At worst, the instruction misstated the law. On its own, the "cessation of employment"—the state of affairs in which the employment relationship has ended (or, with certain facts, paused)—does not rescind the employer's authorization, as employment can cease without any action whatsoever from the employer. And there is not "a high probability that the erroneous instruction did not affect the outcome of the case." *O'Brien*, 57 F.4th at 121 (cleaned up). To the contrary, it is highly probable the erroneous instruction affected the outcome because it permitted the jury to convict Eddings on the Government's only theory of the case.

At best, the District Court's instruction was liable to confuse the jury. There may be facts in some hypothetical case in which a jury could find "the cessation of employment rescinds authorization," like facts indicating the employer terminated the employment relationship and, along the way, revoked the employee's permission to continue to access its computers. But again, this instruction allowed the jury to convict without any finding PCF did anything to withdraw its authorization. The instruction opened the door for the jury to find Denis accessed Rodin's account without authorization simply because she accessed it after she resigned. And there is every reason to think the jury walked through that door when there was no evidence PCF took steps of its own to revoke its authorization.

To be sure, the preceding sentence of the instruction might have steered the jury in the right direction by emphasizing that once a computer's owner has authorized someone's access, subsequent access is "without authorization" only if "the person who controls the right of access to the computer has withdrawn or rescinded permission to use the computer and the person uses the computer anyway." However, we "cannot assume that the jury will have the wherewithal to heed that part of the instruction that is accurate and disregard that which is not." *Dressler v. Busch Ent. Corp.*, 143 F.3d 778, 783 (3d Cir. 1998). "Rather, we must assume that[,] if the jurors are provided instructions that are partly flawed[,] they may well choose the flawed part to inform their duties as finders of fact." *Id.*

By either standard, the jury instruction warrants vacating Eddings's conviction.

C. The District Court did not err in denying Eddings's motion for a new trial to redress the Government's remarks about extortion.

Last, Eddings argues she deserved a new trial because a prosecutor briefly suggested the Government would have charged her with extortion if PCF had met her demand for payment. The remarks may have been improper. Even so, they were harmless.

When a defendant seeks a new trial because of a prosecutor's closing remarks, we "first determine whether the remarks were improper." *United States v. Savage*, 85 F.4th 102, 124 (3d Cir. 2023) (citing *Zehrbach*, 47 F.3d at 1264). If so, we assess them for harmless error. *Id.* (quoting *Zehrbach*, 47 F.3d at 1264). In making that determination, "we consider 'the scope of the objectionable comments and their relationship to the entire proceeding, the ameliorative effect of any curative instructions given, and the strength of the evidence supporting the defendant's conviction.'" *Id.* (quoting *Zehrbach*, 47 F.3d at 1265). We reverse the District Court's denial of the motion if, but only if, improper remarks prejudiced the defendant. *Zehrbach*, 47 F.3d at 1265.

The prosecutor's comment about why the defendants were not charged with extortion may not have been appropriate. He purported to inform the jury of a matter not in evidence. *See id.* at 1266. But it did no harm here. First, in the scope of the proceedings, the remarks were brief: two sentences among about 50 pages of closing arguments. *See Savage*, 85 F.4th at 124 (no prejudice from two lines in a 277-page closing argument); *Zehrbach*, 47 F.3d at 1260, 1267 (no prejudice from two sentences in a 40-page closing argument); *United States v. Homer*, 545 F.2d 864, 868 (3d Cir. 1976) (no prejudice from two paragraphs in a 60-page closing argument).

Second, the prejudicial power of the remarks was limited by their terms. To be sure, the prosecutor suggested to the jury the defendants would have been charged with extortion had they wrung any money from PCF. But he expressly reminded the jury the defendants were not charged with extortion. And he explained the limited role the evidence of their profit motive should have in the case: establishing the intent element of the CFAA felonies for which they were charged.

Third, the District Court issued a curative instruction that we repeat:

> Extortion is not, repeat, not a part of this case. The defendants are not charged with extortion. You are not to consider that subject in your jury deliberations. Why a charge of extortion was not brought is not relevant and not to be considered . . . and any argument[] by any of the lawyers or any of the parties in this case about that subject is to be disregarded by you.

SAppx1002. Then the Court reiterated a complementing instruction it had issued at the outset of the trial: the jury must decide based on the evidence, and the closing arguments were not evidence. "A jury is presumed to follow a court's instruction to disregard inadmissible evidence inadvertently presented to it, 'unless there is an "overwhelming probability" that the jury will be unable to follow the court's instructions, and a strong likelihood that the effect of the evidence would be "devastating" to the defendant.'" *Savage*, 85 F.4th at 125 (quoting *Greer v. Miller*, 483 U.S. 756, 766 n.8 (1987)). Eddings has given us no reason to doubt this jury could follow these instructions.

Together, the brevity and limitations of the prosecutor's remarks and the District Court's incapable-of-being-misunderstood curing instructions render the remarks harmless. *See id.* at 124–25 (holding, in light of similar considerations, a defendant was not prejudiced by prosecutor's closing accusation he committed a murder with which he was not charged). The Court did not abuse its discretion in refusing to grant Eddings a new trial to redress them.[6]

[6] One other matter merits mention. Before the District Court, Eddings's counsel filed a brief that included a misleading quotation. Counsel claimed the quotation was from *Brekka*, but it was really from a district court opinion glossing *Brekka* in a manner helpful to Eddings's position. The Court admonished him. Then, in briefing before us, he included the same passage and misleading citation. We asked him to show cause why he should not be sanctioned. The truculent response he filed did not help. At oral argument, however, counsel accepted sole

*   *   *

We have cautioned that the CFAA can "become[] a hammer in search of a nail." *NRA*, 154 F.4th at 158. This is another such case. The statute prohibits accessing a computer "without authorization." 18 U.S.C. § 1030. Its primary target is hackers. *See Van Buren*, 593 U.S. at 389. Eddings was convicted because her friend, Denis, accessed her employer's email account after resigning from her job. But Denis's employer had not rescinded the permission it gave her to access the account. Nor had her employer conditioned its permission on her tenure in the job. So Denis did not access it without authorization. We do not condone the conduct of either Denis or Eddings. Far from it. But we hold that, on this record, Eddings did not violate § 1030. We therefore vacate her conviction and remand with instructions to enter a judgment of acquittal.

personal responsibility. We will let the matter pass without sanction.

MONTGOMERY-REEVES, *Circuit Judge*, dissenting.

This appeal concerns the Computer Fraud and Abuse Act (the "CFAA"). 18 U.S.C. § 1030. A defendant violates the CFAA if she "intentionally accesses a computer without authorization or exceeds authorized access[] and thereby obtains . . . information from any protected computer." *Id.* § 1030(a)(2). We must determine what "without authorization" means. More specifically, we must determine whether a former employee—who once enjoyed authorization—may lose authorization by resigning from her employment, or if the authorizing party must always proactively rescind her authorization. I see nothing in the CFAA's text, its context, its legislative history, or in the case law interpreting the statute, that *requires* employer rescission to terminate "authorization" (the "Express Rescission Requirement").[1] Instead, both employee resignation and employer rescission are facts a jury may consider in determining whether authorization exists. Thus, I must respectfully dissent.

First, the text. When interpreting statutory terms, we "presume that words carry their ordinary meaning," and we

[1] The Majority Opinion notes that the record contains no evidence of any contract governing Denis's authorization to use the account. Presumably, the Majority Opinion might come out differently if such contractual language existed. In my view, contractual language that stipulates when rescission occurs still entails express rescission because imposing such a contractual limitation requires express action by the authorizing party; the express action just occurs at the beginning of the legal relationship, rather than the end. Thus, I include this caveat in my understanding of the Express Rescission Requirement.

look to "standard reference works such as legal and general dictionaries" to determine their ordinary meaning at that time. *United States v. Caraballo*, 88 F.4th 239, 246 (3d Cir. 2023) (quotations omitted). "Without" means "not having," to be "devoid of" or in "absence of." *Without*, CONCISE OXFORD ENGLISH DICTIONARY (7th ed. 1982).[2] And "authorize" means "[t]o empower; to give a right or authority to act. To endow with authority or effective legal power, warrant, or right. To permit a thing to be done in the future . . . implying a direction to act." *Authorize*, BLACK'S LAW DICTIONARY (5th Ed. 1979) (internal citation omitted). In sum, "without authorization" means to be lacking or devoid of approval or permission.

Absent from these definitions is any suggestion that an authorizing party, like the employer in this appeal, must communicate to an authorized party that authorization is rescinded for it to be so. Instead, the definition of the phrase encompasses a broad spectrum of facts. For example, rescission could be express if an authorizing party—like an employer—affirmatively communicates to an authorized party through their words or conduct that authorization has been rescinded. But a termination could also be implied by factual

[2] Merriam Webster's New Collegiate Dictionary also defines "without" as "a function word . . . indicat[ing] the absence or lack of something." *Without*, WEBSTER'S 9TH NEW COLLEGIATE DICTIONARY (9th ed. 1983).

circumstances[3] or completion of a legal obligation.[4] The definition of authorization does not foreclose any of these

[3] Consider the following example of implied termination by factual circumstances. In 2021, a boyfriend gives his then-girlfriend a password to his personal email and authorizes her to use it for the limited purpose of sending a party invite to their friends. She does so. Years pass, and the two part ways. The girlfriend then discovers the boyfriend's password is still saved in her browser. There is evidence that the girlfriend knew that the two were no longer together and that she understood she likely did not have permission to use the boyfriend's email. She nonetheless logs into his email, obtains several of the boyfriend's personal documents, and uses them to attempt to harm him because of the pain he caused her. A jury could conclude that the girlfriend's access was unauthorized because it impliedly terminated upon the girlfriend's conclusion of the task for which the boyfriend granted authorization.

[4] Consider the following example of implied termination by legal operation. A celebrity hires an IT contractor to work on her computer. The parties sign a contract that only details the job to be done and the amount to be paid. The contractor operates remotely, so the celebrity provides him with her password. The IT contractor successfully completes his work after remotely entering the celebrity's computer. Eight weeks later, the contractor accesses the celebrity's computer, obtains highly sensitive and embarrassing materials, and threatens to sell the materials to the press. A jury could conclude that the IT contractor was not authorized to access the celebrity's computer after completion of the legally agreed-to task and therefore his authorization was terminated by legal operation.

factual scenarios.

Second, nothing in the statutory context supports the Express Rescission Requirement. The CFAA never suggests that we *must* look to an authorizing party's behavior to determine whether "authorization" has terminated. *See generally* 18 U.S.C. § 1030. And terms like "rescission" or "revocation"—which might suggest we need to assess an authorizing party's actions—do not appear in the statute. *See id.* So I see no suggestion that Congress limited the CFAA's reach to incidents where an authorizing party expressly rescinds authorization.

Third, the legislative history does not support narrowing its coverage through the Express Rescission Requirement. Congress passed the first iteration of what is now the CFAA in 1984 with the goal of addressing "'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015) (quoting H.R. Rep. 98-894, at 6, 11 (1984)). At the forefront of their concern was *privacy* or preventing any unwanted invasion by any unwanted actor. *See* S. Rep. 99-432, at 6–7 (1986) (noting that the "premise of [18 U.S.C. § 1030(a)(2)] is *privacy protection*" and, therefore, even terms like "obtain" should be broadly construed as the "mere observation of data" (emphasis added)). And in the years since 1984, Congress has consistently broadened the statute's reach to capture more conduct.[5]

Congress's broad conception of the conduct it hoped to capture is evinced by examples of unauthorized conduct that motivated the CFAA's enactment. For example, one motivating case—discussed by Congress—is strikingly similar to ours. There, an "owner of a computer company stole confidential software by tapping into the computer system of a previous employer from [the] defendant's remote terminal." H.R. Rep. 98-894, at 6. Conspicuously absent from Congress's presentation of the offending conduct is *how* the previously-authorized party came to be separated from his previously-authorizing employer. In my view, Congress omitted these details because it did not understand the conduct of authorizing parties to always be dispositive of whether authorization exists. Had Congress understood there to be an Express Rescission Requirement, it presumably would have noted how

[5] 18 U.S.C. § 1030(a)(2) (1984) (restraining § 1030(a)(2) to only those that "intentionally access[] a computer without authorization or exceed[] authorized access, and . . . obtain[] information contained in a financial record of a financial institution, or of a card issuer . . ., or contained in a file of a consumer reporting agency on a consumer"); 18 U.S.C. § 1030(a)(2) (1996) (adding to the list of protected information "information from any department or agency of the United States" and "information from any protected computer if the conduct involved an interstate or foreign communication"); 18 U.S.C. § 1030(a)(2) (2008) (modifying "information from any protected computer if the conduct involved an interstate or foreign communication" to simply "information from *any protected computer*").

authorization terminated in its recitation of the offending conduct. Or even better, a limitation would have appeared in the statute itself. In all, the legislative history suggests that Congress intended § 1030(a)(2) to cover a broad scope of conduct, not to narrowly apply only after express rescission by an authorizing party.[6]

Fourth, and finally, no case law in or outside of this Circuit dictates a different result. Only two relevant binding decisions tangentially relate to the meaning of "without authorization": *Van Buren* and *Durenleau*. Both cases involve a current employee operating *with* authorization. *Van Buren v. United States*, 593 U.S. 374, 382 (2021); *see NRA Grp., LLC v. Durenleau*, 154 F.4th 153, 168–69 (3d Cir. 2025). Neither case purports to define "without authorization"; nor does either case engage in any meaningful analysis that helps us define the contours of what it means to operate "without authorization."

The Ninth Circuit has more specifically dealt with the statutory phrase "without authorization." It first addressed the phrase in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132–33 (9th Cir. 2009). There, the Ninth Circuit held that an individual acts "without authorization" "when [a] person has not received permission to use [a] computer for any purpose

[6] I acknowledge, like the Majority Opinion identifies, that construing "without authorization" too broadly triggers important policy concerns. But in my view, these concerns are obviated by § 1030(a)(2)'s state-of-mind requirement. *See* 18 U.S.C. § 1030(a)(2) ("Whoever . . . *intentionally* accesses a computer without authorization. . ." (emphasis added)); *Durenleau*, 154 F.4th at 168 n.7 (recognizing that "intentionally" in § 1030(a)(2) modifies the phrases that follow it, including "without authorization").

(such as when a hacker accesses someone's computer without any permission), ***or*** when the employer has rescinded permission to access the computer and the defendant uses [it] anyway." *Id.* at 1135 (emphasis added). The *Brekka* court did not articulate how an employer must rescind permission, but it noted—without holding—that if an authorized party accessed certain information "after he left the company," there would be no dispute that he "accessed a protected computer 'without authorization' for purposes of the CFAA." *Id.* at 1136.

Seven years later, in the same week, the Ninth Circuit issued two more opinions expounding upon *Brekka*. In *Facebook, Inc. v. Power Ventures, Inc.*—a non-employment-related case—the Ninth Circuit read *Brekka* as holding, not just suggesting, that a former employee acted "without authorization" when he "accessed a protected computer" "after he left the company." 844 F.3d 1058, 1066 (9th Cir. 2016) (quoting *Brekka*, 581 F.3d at 1136). *Facebook*, like *Brekka*, never mentions an authorizing party's behavior.

In *United States v. Nosal*, the Ninth Circuit held that "[i]mplicit in the definition of authorization is the notion that someone . . . can grant or [rescind] . . . permission." 844 F.3d 1024, 1035 (9th Cir. 2016) (emphasis added) ("*Nosal II*"), *overruled on other grounds by Lagos v. United States*, 584 U.S. 557 (2018). The *Nosal II* court then turned to the specific facts of that case, acknowledged that the authorized party received particularized notice of his rescinded access, and held that the authorized party acted "without authorization." *Id.* at 1036. In other words, the *Nosal II* court relied on the specific facts of that case. It did not hold that the government *must* show employer rescission in every employment-related CFAA case.

The most I can deduce from the text, statutory context, legislative history, and relevant case law is that a jury can consider an authorizing party's actions when determining whether an authorized party acted "without authorization." But such acts are not mandatory. I would affirm because the District Court correctly allowed a jury to consider whether the cessation of employment impliedly rescinded authorization in this case. Thus, I respectfully dissent.