3rd Circ. Ruling Forces A Shift In Employer CFAA Probes

By **David Lashway, Philip Robbins and Brad Carney** (October 17, 2025)

David Lashway

Philip Robbins

Brad Carney

On Aug. 26, the U.S. Court of Appeals for the Third Circuit issued a consequential decision in NRA Group LLC v. Durenleau, significantly narrowing employers' recourse under the Computer Fraud and Abuse Act, or CFAA.

The court, relying heavily on the U.S. Supreme Court's 2021 decision in Van Buren v. U.S., held that employers cannot bring claims under the CFAA against employees who misuse information they are authorized to access unless they explicitly breach technical or code-based barriers such as firewalls.

Additionally, the court held that passwords protecting proprietary business information, alone, do not constitute trade secrets under federal or Pennsylvania law.

This decision reshapes the landscape for internal investigations, effectively limiting the reach of the CFAA as one of the primary tools for addressing many insider threats.

While CFAA-based claims remain relevant in scenarios involving explicit hacking or circumvention of technical security measures, organizations must carefully assess each claim and may have to rely on additional legal tools — such as breach of contract, trade secret laws, fiduciary duty claims and state-level statutes — as a mechanism for recourse.

Corporate counsel and cybersecurity teams may therefore consider recalibrating their investigation strategies to account for these alternative approaches as well as reviewing their information security policies, procedures and technical controls in light of Durenleau.

Legal Implications and Practical Applications

The case arose from an employer's claims under the CFAA and trade secret law, following two employees' unauthorized sharing of a password spreadsheet and subsequent access to company systems.

While this conduct violated internal company policies, the employees did not circumvent any technical security barriers.

The Third Circuit's ruling depended substantially on the Supreme Court's decision in Van Buren, applying a gates-up-or-down inquiry, to conclude that the employees' actions did not exceed authorized access or constitute access to a protected computer system without authorization in the absence of any "evidence of code-based hacking," according to the Third Circuit's decision.

The Third Circuit's interpretation aligns with U.S. Court of Appeals for the Ninth Circuit's 2012 decision in U.S. v. Nosal,[1] as well as the U.S. Court of Appeals for the

Fourth Circuit's 2012 decision in WEC Carolina Energy Solutions LLC v. Miller,[2] stating that the CFAA does not countenance claims premised on a breach of workplace computer-use policies by current employees, absent evidence of hacking.

The court further rejected broad readings of the CFAA's criminal provisions, cautioning against turning "commonplace, day-to-day policy violations," into criminal acts, and partially quoted prior precedent, adding that the court treads "carefully, mindful of the 'canon of strict construction of criminal statutes.'"

While Van Buren had already adopted the gates-up-or-down rule, the Supreme Court stopped short of deciding whether authorization might still be cabined by contracts or policies rather than just technical barriers.

Durenleau addresses that gap, standing for the proposition that "unauthorized access" under CFAA requires code-based hacking, not simply violating internal use restrictions.

This clarification is particularly important given legal scholar Orin Kerr's observation in a 2010 article published in the Minnesota Law Review that "cases applying the CFAA to allegedly disloyal employees have become by far the most common type of CFAA case."[3]

Notably, the court explicitly referenced alternative mechanisms employers have at their disposal to handle employee misconduct, stating that there are "many other causes of action — breach of contract, business torts, fraud, negligence — that provide a remedy for employers when employees grossly transgress computer-use policies. The CFAA is the wrong tool."

Nonetheless, careful application of the facts and consideration of the CFAA remain relevant to any internal investigation as the court clarified that the CFAA still applies to code-based hacking.

Additional Legal Tools

For in-house legal teams and outside counsel tasked with probing insider misconduct, the Third Circuit's opinion signals a strategic shift in how investigations may be executed and resolved.

Particularly, in instances where the investigation determines that no code-based hacking occurred, these teams will need to advise and guide their client, the insider's employer, through alternative means other than the CFAA for seeking recourse.

A few alternative options are further summarized below.

Breach of Contract: NDAs and Acceptable Use Agreements

In the wake of Durenleau, breach of contract claims may become the primary mechanism for employers seeking to hold employees accountable for insider misconduct.

Many companies already require employees to sign confidentiality and nondisclosure agreements, or NDAs, and include computer-use rules in employee handbooks.

When an insider misuses its access and/or data, those agreements can form the basis of a straightforward breach of contract lawsuit.

To strengthen this tool, companies should ensure their agreements explicitly define what constitutes unauthorized access of its systems and unauthorized use or disclosure of company information — e.g., taking data for personal gain, sharing credentials or transferring files to personal accounts.

Clear contractual language puts employees on notice and makes it easier to prove a breach in court. In practice, this means keeping NDAs and acceptable-use policies up to date and obtaining written acknowledgment from employees that they understand and agree to those terms.

While a contract claim may not carry the same teeth as a claim under a federal statute, it offers a reliable path to damages for any provable losses.

Trade Secret Law: The DTSA and State UTSA

When an employee steals or misuses sensitive business information, the federal Defend Trade Secrets Act, or DTSA,[4] and parallel state trade secret statutes may provide an additional mechanism for recourse.

These laws provide strong remedies, including potential seizure orders and exemplary damages,[5] if the information at issue qualifies as a "trade secret," meaning it derives independent economic value from being secret and the company took reasonable steps to keep it secret.[6]

In many insider theft cases, this is a viable claim as customer lists, product designs, business strategies, source code and other proprietary data can be trade secrets if properly protected. Indeed, employers frequently pair CFAA claims with trade secret claims when taking legal action against a rogue ex-employee.[7]

However, Durenleau illustrates a key limitation: Not everything a company considers confidential will meet the trade secret definition.

In Durenleau, the employee allegedly misappropriated a spreadsheet of passwords — something the employer argued was sensitive, but the court held that it did not count as a trade secret because the passwords themselves had no independent economic value.

The passwords were merely keys to other data, and the company did not allege any proprietary algorithm or formula behind them.

The court's message was that it is what the passwords protect, not the passwords themselves, that might be valuable.[8]

To further enhance potential claims under these laws, in-house counsel should coordinate with information technology and management to identify the crown jewels of data that merit trade secret status and ensure the company is implementing requisite security measures, such as encryption, need-to-know access, and employee training.

State Computer Crime and Data Misuse Statutes

State law equivalents to the CFAA may also provide an avenue for recourse through an unauthorized use mechanism. Many states have their own computer fraud or data theft statutes that provide for civil lawsuits or additional criminal penalties.

Some of these laws define "unauthorized access" more broadly than the post-Van Buren CFAA. These laws utilize a use-centric standard that can attach even when a user logs in with valid credentials and never circumvents a gate, but where an employer withheld or withdrew permission to take or use the specific data at issue.

For example, New Jersey's 1984 Computer Related Offenses Act makes it unlawful to purposely or knowingly and without authorization take or alter any data from a computer system.[9]

Likewise, California's 1984 Comprehensive Computer Data Access and Fraud Act imposes both criminal and civil liability where a person "knowingly accesses and without permission ... takes, copies, or makes use of any data."

State computer crime laws like those in New Jersey and California give plaintiffs a use-based path that remains open when no gate was circumvented.[10]

Drafting Effective Policies

The Durenleau decision underscores the importance of tightening internal policies and increasing employee education as preventative measures against misuse. In light of the ruling, employers may consider, among other things, the following.

Clearly Defining Authorized vs. Unauthorized Access

Consider policies that spell out what employees are authorized to access and for what purposes, versus what is off-limits, before access is authorized.[11] Ensure employees are on notice that, even where technical access to certain information is granted, using it beyond their job duties is strictly prohibited.

Obtaining Consent to Monitoring

Consider including explicit language in handbooks and agreements that employees have no expectation of privacy on company systems, and have employees consent to monitoring of their digital activities.[12] This not only helps deter wrongdoing but also ensures the company can collect evidence of any misuse with minimal legal hurdles.

Keeping Policies and Agreements Up to Date

Regularly, and at least annually, consider a review and update of confidentiality agreements, NDAs, and acceptable-use policies to address new technologies and threats, such as generative AI and large language models.[13] Require employees to reacknowledge key policies periodically, creating a record that they are aware of the latest rules.

Implementing an Insider Threat Program

Consider establishing a formal insider-threat management team or program that brings together human resources, IT and legal to assess risks, monitor for red flags and respond swiftly to any suspected internal theft.

A coordinated program can assist in rapid detection of issues early during an incident and ensure a unified, lawful response when policies are violated.

Security and IT Best Practices

Observing that robust technology controls operate in tandem with legal and policy measures, companies have implemented system-hardening measures that both inhibit threat-actor data exfiltration and establish the gates distinguishing authorized use from technical circumvention.

Government agencies and certain cybersecurity vendors identify the following as relevant best practices.

Identity and Access Management

Implement least-privilege access principles.[15] Use just-in-time elevation.[16] Promptly revoke access upon employee separation, and systematically monitor privileged accounts for unusual activity.

Data Loss Prevention

Establish and deploy strong technical gates,[17] such as phishing-resistant multifactor authentication and role-based access controls.[18]

Employ endpoint and email data loss prevention solutions configured to flag uploads to personal cloud services, mass data exports and atypical attachment behaviors, particularly tuned for high-value data repositories.

Monitoring and Logging

Centralize and retain logs of authentication events, file access and egress for investigative purposes.[19] Where possible, logs should be associated with user identities, specific devices, and individual sessions to facilitate rapid and effective incident response.

BYOD Policies

Enforce mobile device management protocols on all personal devices accessing corporate resources, ensuring users provide explicit consent for remote device wiping to help safeguard sensitive data.[20]

Remote-wipe capabilities should form part of a layered security approach, recognizing that reliance solely on remote wiping is insufficient, as devices may be compromised or disabled before receiving wipe commands.

Third-Party Risk Management

Extend confidentiality, access control, monitoring, auditing and cooperation obligations to third-party vendors.[21] Incorporate contractual terms mandating vendor cooperation during investigations and prompt notification requirements in the event of a suspected incident or breach.[22]

Conclusion

Durenleau illustrates that under the CFAA, unauthorized access requires bypassing technical barriers rather than simply violating company policies using valid credentials.

This builds on the gates-up-or-down test introduced in Van Buren. In doing so, the Third Circuit situates the CFAA within a narrower technically defined domain, preserving its applicability in cases involving hacking or bypassing of code-based restrictions and restricting its applicability to workplace disputes centered on policy breaches.

Therefore, employers may need to turn to contractual, trade secret and state-level computer misuse claims as mechanisms to address the broader spectrum of insider misconduct beyond the CFAA's narrowed scope.

David Lashway is a partner and co-chair of the global privacy and cybersecurity practice at Sidley Austin LLP.

Philip Robbins is an associate at the firm.

Brad Carney is an associate at the firm.

Sidley partners John Woods Jr. and Jonathan Wilan contributed to this article.

[1] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

[2] WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012).

[3] https://www.minnesotalawreview.org/wp-content/uploads/2012/03/Kerr_MLR.pdf.

[4] https://www.govinfo.gov/content/pkg/PLAW-114publ153/pdf/PLAW-114publ153.pdf.

[5] https://www.congress.gov/committee-report/114th-congress/senate-report/220/1.

[6] https://www.thesedonaconference.org/sites/default/files/1-1_Sedona_WG12_Identification_of_Trade_Secrets_Oct_2020_ed.pdf.

[7] E.g., https://www.law360.com/articles/2322120/realtor-com-parent-drops-trade-secrets-suit-against-costar; https://www.law360.com/articles/1596492/printing-co-hit-with-5m-ip-verdict-after-ennis-acquisition.

[8] https://www.aberlawfirm.com/wp-content/uploads/2011/03/Almeling.pdf.

[9] https://law.justia.com/codes/new-jersey/title-2a/section-2a-38a-3/.

[10] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=502.&lawCode=PEN.

[11] NIST.SP.800-53r5.pdf" rel="noopener noreferrer" target="_blank">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[12] https://www.cisa.gov/sites/default/files/2024-11/Nine%20Elements%20and%20an%20Example%20for%20Notice%20and%20Consent%20Logon%20Messages%20-%20Contractor%20Owned%20or%20Operated%20Federal%20Information%20Systems.pdf.

[13] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.

[14] https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.

[15] https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege.

[16] https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/just-in-time-access/.

[17] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[18] https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf.

[19] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-92r1.ipd.pdf.

[20] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf.

[21] https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025/.

[22] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.