Third Circuit Aligns With the Supreme Court's Limit on the Scope of the Computer Fraud and Abuse Act

Sep 23, 2025

Categories:

Policies and Handbooks

Authors:

Andrew F. Beck

Does an employee logging into the computer of an employee away from the office, at the request of said employee, to access a document and email it to the employee away from the office constitute criminal behavior under the Computer Fraud and Abuse Act, 18 U.S.C. §1030 (CFAA), a federal statute that imposes criminal penalties and provides for a civil cause of action against individuals who obtain information from a computer by intentionally accessing the computer without authorization or by exceeding authorized access? Also at issue is whether passwords constitute trade secrets under federal and applicable state trade secrets law.

In its recent opinion in *NRA Grp., LLC v. Durenleau*, the Court of Appeals for the Third Circuit adopted the United States Supreme Court's holding in *Van Buren v. United States* regarding the scope of the CFAA's "exceeds authorized access" clause. In *Durenleau*, the Third Circuit held that while these types of actions by employees may violate an employer's workplace computer-use policy, infractions of this nature do not rise to the level of federal crimes under the CFAA.

Background

In January 2021, while employed with the debt-collection firm, National Recovery Agency (NRA), Nicole Durenleau, NRA's Senior Manager of Compliance Services, was out sick due to COVID-19. While out of the office, an urgent request was brought to Durenleau's attention for which she needed a work document but had no means to access it from home due to NRA's restrictions on the ability to access its systems when not physically present in the office. Durenleau was not given a laptop to access NRA's systems while at home and only had access to her work email through her personal phone. As a result, Durenleau gave fellow NRA marketing

employee, Jamie Badaczewski, express permission to use her NRA system credentials to log into NRA's network as Durenleau. Badaczewski then accessed the document Durenleau was in need of – a spreadsheet with Durenleau's passwords – and gave Durenleau the information she needed. The next day, Badaczewski logged into the NRA network as Durenleau again, but this time she emailed the spreadsheet to Durenleau. The actions by both employees, along with Durenleau's creation of the spreadsheet, violated NRA's workplace computer-use policies.

Durenleau eventually resigned in February 2021, and Badaczewski was fired shortly thereafter for her actions in accessing Durenleau's computer and providing her the spreadsheet of passwords. Soon after, NRA brought suit against the two former employees arguing that these actions exceed their authorized use under the CFAA, which 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."

The Third Circuit's Opinion

In an opinion authored by Judge Thomas L. Ambro, the Third Circuit agreed with the District Court's ruling that Durenleau and Badaczewski did not "exceed authorized access" under the CFAA. The court stated that the United States Supreme Court's holding in *Van Buren v. United States* compelled affirming the District Court's ruling. In *Van Buren*, the Supreme Court reasoned 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*." (Emphasis in original). The Supreme Court adopted this position based upon a "gates-up-or-down inquiry," meaning that an individual has the ability or inability to access a computer system, as well as certain areas within a computer system. This inquiry serves to distinguish between actions involving permitted access and hacking (entry without access). Prior to addressing Durenleau and Badaczewski's actions, the Third Circuit noted *Van Buren's* stance that a "mere violation of 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.'"

The Third Circuit applied *Van Buren* to Durenleau and Badaczewski's actions and reasoned that the "gates" of access were "up" for both employees as neither had hacked into NRA's computer systems since they were given access to these systems by virtue of being NRA employees. The court adopted the District Court's position that "an employee is 'authorized to access a computer when his employer approves or sanctions his admission to that computer" (quotation omitted) and determined that NRA authorized both employees to access its computers upon hiring. In holding that these employees did not "exceed authorized access" under the CFAA, the court made clear that while their actions contravened NRA's workplace computer-use policies, they did so with access to NRA's computer system. Specifically, Durenleau's access permitted her to log into her computer and create the spreadsheet in question, and Badaczewski had access to NRA's system because she had been given permission by Durenleau.

NRA also argued that (1) Durenleau was blocked from accessing the NRA system while she was home via NRA's firewalls, and thus she was not authorized to access the system; (2) Badaczewski was not authorized to access Durenleau's files; and (3) Durenleau could not give Badaczewski authorization as she did not have any authorization herself at this time. Unconvinced by these arguments, the court held "absent evidence of code-based hacking, the CFAA does not countenance claims premised on a breach of workplace computer-use policies by current employees." In support of its reasoning, the court opined that it was "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." Ultimately, the court affirmed the District Court's grant of summary judgment in favor of Durenleau and Badaczewski on NRA's CFAA claims. However, it did note other causes of action employers can look to instead of the CFAA to remedy policy violations, including breach of contract, business torts, fraud, and negligence.

NRA also brought a claim against the two employees under the federal Defend Trade Secrets Act (DTSA) and Pennsylvania Uniform Trade Secrets Act (PUTSA), specifically claiming that the passwords on Durenleau's spreadsheet were trade secrets since the databases accessible through the accounts on the spreadsheet contained consumer identifiable and other private information. As such, NRA argued that Durenleau's creation of the spreadsheet and Badaczewski's emailing it to Durenleau constituted misappropriation of trade secrets in violation of the DTSA and PUTSA. In holding that the passwords in question were not trade secrets, the court determined that (1) passwords are merely random combinations of letters and numbers serving as a roadblock to other proprietary information; (2) passwords have no *independent* economic value in the way a customer list may have; and (3) passwords are not trade secrets if they are not created through any special formula or algorithm. (Emphasis in original).

The court also affirmed the District Court's grant of summary judgment in favor of Durenleau and Badaczewski on NRA's state law claims for civil conspiracy and breach of common-law duty of loyalty. As for the civil conspiracy claim, the court held that (1) there was no free-standing cause of action to support the claim as Durenleau and Badaczewski did not violate the CFAA, DTSA, or PUTSA; and (2) NRA could not demonstrate malice, a necessary and crucial element to a civil conspiracy claim. In rejecting NRA's breach of the duty of loyalty claim, the court held that NRA could not prove that Durenleau and Badaczewski did not act in NRA's best interest, as the sole use of the information accessed was to resolve an urgent issue for NRA.

Conclusion

Ultimately, the *Durenleau* decision reinforces *Van Buren's* limitation on an employer's ability to pursue CFAA claims against employees and maintains that this statute is not the avenue for employers to follow in seeking remedies for violations of workplace computer-use policies. This decision serves as a reminder for employers to review their existing computer-use policies to ensure access to various electronic information is authorized to only those employees that

require certain access. In light of *Van Buren* and *Durenleau*, employers should also review their policies related to the confidentiality of business information to ensure these policies are sufficiently tailored to provide adequate protection for confidential information.

FBT Gibbons