Proskauer

District Court Decision Brings New Life to CFAA to Combat Unwanted Scraping

New Media and Technology Law Blog on **November 10, 2022**

On October 24, 2022, a Delaware district court held that certain claims under the Computer Fraud and Abuse Act (CFAA) relating to the controversial practice of web scraping were sufficient to survive the defendant's motion to dismiss. (*Ryanair DAC v. Booking Holdings Inc.*, No. 20-01191 (D. Del. Oct. 24, 2022)). The opinion potentially breathes life into the use of the CFAA to combat unwanted scraping.

In the case, Ryanair DAC ("Ryanair"), a European low-fare airline, brought various claims against Booking Holdings Inc. (and its well-known suite of online travel and hotel booking websites) (collectively, "Defendants") for allegedly scraping the ticketing portion of the Ryanair site. Ryanair asserted that the ticketing portion of the site is only accessible to logged-in users and therefore the data on the site is not public data.

The decision is important as it offers answers (at least from one district court) to several unsettled legal issues about the scope of CFAA liability related to screen scraping. In particular, the decision addresses:

- the potential for vicarious liability under the CFAA (which is important as many entities retain third party service providers to perform scraping)
- how a data scraper's use of evasive measures (e.g., spoofed email addresses, rotating IP addresses) may be considered under a CFAA claim centered on an "intent to defraud"
- clarification as to the potential role of technical website-access limitations in analyzing CFAA "unauthorized access" liability

To find answers to these questions, the court's opinion distills the holdings of two important CFAA rulings from this year – the Supreme Court's holding in *Van Buren* that adopted a narrow interpretation of "exceeds unauthorized access" under the CFAA and the Ninth Circuit's holding in the screen scraping *hiQ* case where that court found that the concept of "without authorization" under the CFAA does not apply to "public" websites.

Ryanair's complaint advanced multiple claims under the CFAA including, among others:

- 18 U.S.C. § 1030(a)(2)(C), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer,"
- 18 U.S.C. § 1030(a)(4), which prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value."; and
- 18 U.S.C. § 1030(a)(5)(A), which prohibits "knowingly caus[ing] the transmission of a…program… and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." [1]

The defendants argued that Ryanair's complaint must be dismissed for several reasons: (1) that the CFAA does not permit claims to be brought on a vicarious liability theory; (2) that Ryanair has not alleged that the defendants have caused the requisite harm for a viable CFAA claim; (3) that Ryanair did not sufficiently plead its CFAA claim based on an intent to defraud; and (4) that Ryanair's CFAA "without authorization" claim fails on the merits in light of the principles of *Van Buren* and *hiQ*.

Vicarious liability under the CFAA

According to the plaintiff's amended complaint, the defendants entered into numerous contracts with non-party scraping providers to bypass the technical and non-technical barriers on the Ryanair site and perform the scraping at issue. Ryanair's complaint asserts that "Defendants cannot avoid CFAA liability by engaging agents and third parties to exceed the Defendants' authorized access to the Ryanair Website on their behalf."

The defendants argued that Ryanair could not rely on a theory of indirect or vicarious liability in bringing a civil claim under the CFAA, contending that the statute permits a civil action "against the violator," that is, the individuals who actually take the actions at issue. Ryanair contended that CFAA liability extends beyond the persons who directly access a computer unlawfully and to those who direct, encourage, or induce a third party to commit such violation.

In finding Ryanair's vicarious civil claims were cognizable under the CFAA, the district court pointed to a bevy of decisions that have recognized that vicarious or indirect liability under the CFAA extends to parties who direct, encourage, induce, or conspire with others to commit acts that violate the statute. While the court conceded that there is a body of case law that stands for the more limited proposition that a principal is not vicariously liable for an agent's CFAA violation if the principal had no knowledge of or involvement in the agent's conduct, the court found in the instant case that Ryanair alleged that the defendants directed third parties to access the myRyanair portion of the Ryanair website without authorization, and therefore would have had the requisite knowledge. Moreover, the court noted that Ryanair allegations that defendants "entered into written agreements with their agents and certain third parties who access the Ryanair Website without authorization (or alternatively, in excess of their authorized access) on behalf of the Defendants" supported a plausible vicarious claim. As such, the district court found that a vicarious liability claim under the CFAA was adequately pleaded at this stage.

CFAA "Intent to Defraud" Claim Based on Evasive Scraping Practices

Ryanair's complaint alleges a violation of 18 U.S.C. § 1030(a)(4), which prohibits "knowingly and with an intent to defraud access[ing] a protected computer without authorization." Examining the issue of whether the federal Rule 9(b) heightened pleading standards for fraud claims apply to this type of CFAA claim, the court declared that "the law on this issue is a mess." Sidestepping the question, the court found Ryanair's CFAA "intent to defraud" claim to be sufficiently pleaded under any standard, concluding that the complaint sufficiently alleged that the defendants "engaged in fraudulent conduct by misrepresenting themselves, for example by 'lying about [their] email address[es] or anonymizing [their] IP address[es],' when creating accounts on the Ryanair website" and using fake user names to avoid detection from Ryanair's anti-bot programs.

Access "Without Authorization": Clarifying *Van Buren*

Contending that Ryanair's "unauthorized access" claim should be dismissed on the merits, the defendants argued that the Ryanair website is a public website, to which the CFAA's concept of "authorization" or "authorized access" does not apply; Ryanair countered that the portion of its website where tickets may be booked is not public and requires a customer login and that, regardless, the defendants were not authorized to access the that portion of the Ryanair website.

Citing the Supreme Court's *Van Buren* decision and the Ninth Circuit's *hiQ* opinion, the Delaware court stated that "recent case law interpreting the CFAA makes clear that the CFAA's concept of authorization focuses heavily on technological barriers to access"[2], an interpretation bolstered by the *hiQ* court's differentiation of a public website and one "protected by [a] username and password authentication system." As the Ryanair court summed up:

> "The above cases make clear that in order for the CFAA's 'without authorization' and 'exceeds authorized access' elements to apply, some sort of authentication mechanism (e.g., the use of usernames and passwords) must be employed to limit access to the website. If the information on the website is publicly available without requiring users to authenticate themselves, a violation of the terms of use or the defiance of a cease-and-desist letter will not give rise to liability under the CFAA.

Thus, for a website to fall under CFAA protections, the court said, it must have erected limitations on access (whereas, if a website is made available to the public without any authentication requirement, the concept of "without authorization" is inapplicable).[3]

Applying these principles, the Delaware court noted that Ryanair alleges that users must login to the myRyanair portion of the Ryanair website using a username and password. Further, Ryanair alleged and that it used technical measures to attempt to block software bots engaging in scraping of the site (measures which were allegedly bypassed by the defendants). Ryanair's amended complaint further alleged that the defendants circumvented code-based authentication mechanisms designed to limit access to the myRyanair portion of the website, in violation of the terms and even after receiving cease-and-desist letters revoking access. As the Ryanair court concluded:

> "Although those allegations would be insufficient to establish liability under the CFAA if the contents of the myRyanair portion of the website were accessible to the public without authentication, courts have found cease-and-desist letters to withdraw authorization to access a protected portion of a website when an authentication mechanism protected access to that portion of the website."

Thus, the Delaware court allowed the "unauthorized access" claims to go forward as Ryanair had raised a plausible claim as to whether the myRyanair portion of its website was non-public, thus making the defendants' continued access to those pages unauthorized for purposes of the CFAA.

Final Thoughts

There are a number of specific and important observations to discern from the decision:

1. The ruling in the *Ryanair* case suggests that a cognizable vicarious liability claim under the CFAA is certainly possible in certain circumstances where the commissioning party has the requisite knowledge and control over the scraper's actions or a party induces another to commit violations of the CFAA. The ruling also suggests that this would be true even in the absence of an agency relationship or, as the *Ryanair* court stated about the defendants' alleged relationships in the instant case, even if an agency relationship is expressly disclaimed in any side agreement between the commissioning party and the data scraper.
2. The court's ruling is notable in that it suggests that a CFAA "intent to defraud" claim might be pleaded based on actions taken by data scrapers to avoid anti-scraping technologies, such as rotating or anonymizing IP addresses, changing user agent information, employing CAPTCHA solvers, or entering false user login information. It remains to be how future courts would characterize specific anti-detection measures under the CFAA.
3. The Supreme Court's *Van Buren* decision left some issues to be further litigated, specifically regarding its description that the clauses of the CFAA should be seen as a "gates-up-or-down" inquiry focusing on whether the "gates" of the computer system were open (i.e., the user in question was permitted access), or whether the "gates" were closed (i.e., the user was not permitted access). But what closes or opens the gates? The *Ryanair* court stated that the inquiry should focus on technical limitations. In the future, if this line of reasoning is followed, CFAA authorization questions may be litigated over what specific technical measures

limiting access are sufficient to lower the gate. In the instant case, the court found that Ryanair's allegations that it required a username/password login before access was granted to certain airline ticketing pages was sufficient to make a colorable "unauthorized access" claim under the CFAA. Under this rationale, the onus is on the website or database operator to place material that it does not want to be deemed "public" and beyond the reach of the CFAA behind an appropriate technical "wall."

---

[1] In quickly dismissing this claim, the court found that while Ryanair did allege technical interference caused by the defendant's scraping, the complaint did not allege that defendants specifically intended to cause any interruptions to the site or damage Ryanair's system.

[2] The Delaware court stated: "Although the Court [in the *Van Buren* case] declined to expressly decide whether that inquiry 'turns only on technological (or 'code-based' limitations) on access, or instead also looks to limits contained in contracts or policies,' the Court's ultimate holding—that a police officer did not violate the CFAA when he accessed police records for an improper purpose—strongly suggests that the operative question is whether a technological or code-based limitation exists to prevent access to a computer by those who do not have proper authorization."

[3] Indeed, in *Van Buren*, the Supreme Court stated that liability under both the 'without authorization' and "exceeds authorized access" clauses stems from 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. When the "gate" is up or down, however, was not fully clarified by the Supreme Court, as it dropped the semi-notorious Footnote 8 in the *Van Buren* opinion, stating: "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." For further discussion of these issues, please see our prior post.

View original.

Related Professionals

- **Jeffrey D. Neuburger**