Bloomberg Law®

Privacy and Security Law Report®

Litigation

The Dark Web—the Next Frontier in Data Breach Standing Analysis Amid a Deepening Circuit Split

Dark Web

A split among U.S. Circuit Courts of Appeals regarding what harm should suffice to maintain standing in data breach litigation doesn't get easier to address as new questions of whether extrinsic evidence from Dark Web searches of breached personal data for sale can be relied on at the motion to dismiss stage of litigation, the authors write.

By Andrew B. Serwin, Purvi G. Patel, and Alexandra Laks

The dark web—the alternative internet of websites often offering illegal products and stolen information for sale—presents complex issues in the context of considering harm in data breach litigation.

Article III standing is one of the most commonly litigated issues in privacy and data breach litigation, and courts disagree about whether an increased risk of identity theft is sufficient to confer standing. The circuit split on the issue has widened over the past year, with the U.S. Court of Appeal for the D.C. Circuit joining the Sixth, Seventh, and Ninth Circuits in finding standing based on increased risk of identity theft, and the Eighth Circuit joining the Third and Fourth Circuits in finding such injury too speculative to warrant standing. The U.S. Supreme Court passed up an opportunity to resolve the split this year in *CareFirst v. Attias*.

Andrew Serwin is a partner in Morrison & Foerster LLP's global privacy and data security practice group in San Diego.

Purvi Patel is a partner in Morrison & Foerster's litigation and privacy and data security practice groups in Los Angeles.

Alexandra Eve Steinberg Laks is an associate in Morrison & Foerster's litigation practice group in San Francisco.

The U.S. District Court for the Western District of New York recently addressed this legal division in *Fero v. Excellus Health Plan, Inc.*, and also relied on extrinsic evidence to find that data breach plaintiffs had standing based on alleged increased risk of harm.

There are two key takeaways from *Fero*:

- **Second Circuit's Position on Article III Standing.** The *Fero* court interprets the Second Circuit's memorandum disposition in *Whalen v. Michaels Stores, Inc.*, which affirmed a district court's decision that a plaintiff lacked standing based on an increased risk of harm because the plaintiff did not allege a threat of future fraud, as indicating that the Second Circuit *would side* with Circuits holding increased risk of identity theft is enough for Article III standing; and
- **Extrinsic Evidence of Risk of Identity Theft.** In relying on extrinsic evidence to establish standing, including Dark Web search results and statements in a forensic report, the *Fero* court potentially opens the door to plaintiffs' reliance on this type of evidence to rebut attacks on standing at the motion to dismiss stage.

We provide further background on the legal issues, the court's decision, and key takeaways below.

The Legal Landscape: Article III Standing in the Data Breach Context

Under Article III of the U.S. Constitution, to maintain a claim in federal court, a plaintiff must have standing. The plaintiff bears the burden of establishing the following three elements:

 ISSN 1538-3423

1. that the plaintiff has suffered an injury in fact—an invasion of a legally protected interest that is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical;

2. that there is a causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and

3. that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[4]

While there have been a number of Supreme Court decisions addressing Article III in the data breach context, *Clapper v. Amnesty International USA* and *Spokeo, Inc. v. Robins* have had the greatest impact.

Clapper In *Clapper*, the Supreme Court examined Article III standing in a matter arising from allegations that certain amendments to the Foreign Intelligence Surveillance Act (FISA) were unconstitutional. The plaintiffs asserted that they had standing to sue because, as a result of the amendments, there was an objectively reasonable likelihood that their communications with foreign contacts would be intercepted in the future. Specifically, they alleged the following causal chain: (i) the Government would likely target their communications; (ii) the Government would choose the specifically challenged method of surveillance; (iii) the FISA court would authorize the surveillance; (iv) the Government would succeed in intercepting their communications; and (v) the plaintiffs would be parties to the communications that the Government intercepts. The plaintiffs also argued that they were suffering present injury based on taking costly and burdensome measures to protect the confidentiality of their international communications.

The Court rejected both arguments. With respect to plaintiffs' alleged future injury, the Court held that, in light of plaintiffs' ''highly attenuated chain of possibilities,'' they ''[could] not demonstrate that the future injury they purportedly fear is certainly impending.'' And with respect to their alleged current injuries, the Court held that plaintiffs could not ''manufacture standing by incurring costs in anticipation of non-imminent harm.'' Plaintiffs accordingly could not establish that their alleged injury in fact was ''fairly traceable'' to the challenged action.

Spokeo In *Spokeo*, the Supreme Court analyzed whether allegations of a statutory violation alone are sufficient to satisfy Article III. The Court ruled that a plaintiff cannot establish standing based on the violation of a statutory right without adequately alleging that the violation caused some concrete harm. The Court, however, also stated that ''[t]he violation of a procedural right granted by statute can be sufficient in *some* circumstances to constitute injury-in-fact.'' In particular, a ''risk of real harm'' may sometimes satisfy the concrete injury requirement. Thus, *Spokeo* required a fact-specific inquiry into the harm caused by a statutory violation.

The Fero Decision The Supreme Court's *Clapper* and *Spokeo* decisions have led federal courts to reach differing conclusions as to what a plaintiff must plead to establish Article III standing. The *Fero* decision, issued by Judge Wolford of the U.S. District Court for the Western District of New York, discusses this split in authority and contributes to the growing body of law on this evolving issue.

In *Fero,* the court considered, on a motion for reconsideration of a motion to dismiss order, whether a certain group of putative class action plaintiffs had alleged sufficient harm arising out of a data breach to establish Article III standing. The plaintiffs alleged that hackers had obtained various forms of personal identification information (PII) and personal health information (PHI) through a cyberattack on defendant Excellus (a health care provider), but they did not allege that they had suffered any misuse of their PII after the data breach.

The *Fero* court originally dismissed these ''non-misuse'' plaintiffs' claims on the ground that their alleged harm from increased risk of identity theft did not meet the injury-in-fact requirement for Article III standing. On reconsideration, however, the court changed its mind. Its decision was based on both evolving law and ''new'' facts.

The Law

Whalen In granting reconsideration, the court relied in part on the Second Circuit's recent unpublished summary order in *Whalen*. The panel in *Whalen* affirmed a district court's dismissal of a data breach claim on standing grounds because the plaintiff had failed to allege a plausible future threat of fraud. In doing so, the Second Circuit ''favorably cited'' a Sixth Circuit case finding that allegations of future harm were sufficient. Although the *Fero* court acknowledged that the summary order in *Whalen* did not have precedential effect and that the standing issue remained unresolved in the Second Circuit, it nonetheless concluded that *Whalen* ''strongly implie[d] that the Second Circuit would follow those circuits that have held that a risk of future identity theft is sufficient to plead an injury in fact.'' As a result, it found reconsideration of its prior dismissal for lack of standing justified.

The Facts—Dark Web Searches and Forensic Report In granting reconsideration, the court also considered the plaintiffs' evidence regarding the Dark Web and a forensic report regarding the alleged ''targeting'' of PII and PHI for sale on the Dark Web.

Specifically, the plaintiffs presented evidence that certain of the non-misuse plaintiffs' PII and PHI was for sale on the Dark Web, including medical records, e-mail addresses, and password account credentials. While a Dark Web search mentioned the Excellus breach, the plaintiffs did not present evidence that the breach was the source of the specific information about the plaintiffs.

The plaintiffs also relied on a post-breach forensic report prepared by a third-party cybersecurity company for the defendant, which the defendants claimed was attorney-work product, but ultimately produced to plaintiffs under a non-waiver agreement. The plaintiffs hired an expert to review the report, who in turn concluded that the purpose of the breach was to collect and sell PII that others could use to commit identity theft.

The court found that the Dark Web search results and the forensic report supported an argument that ''cyber attackers committed the data breach and stole'' the plaintiffs' PII and PHI ''for nefarious reasons and to

  PVLR ISSN 1538-3423

commit identity fraud.'' This evidence, combined with the Second Circuit's decision in *Whalen*, led the *Fero* court to reconsider its prior dismissal of the non-misuse plaintiffs' claims and find standing.

Takeaways *Fero* adds to the deepening circuit split regarding whether allegations of increased risk of identity fraud may satisfy Article III standing requirements. Moreover, the decision is notable in that it relies on extrinsic evidence—Dark Web searches and a forensic report—to reach a conclusion that appears to be inconsistent with the conclusions of *Clapper*. In particular, the court finds standing in the absence of evidence that the alleged breach at issue (as opposed to a different breach) was the source of the information that was allegedly for sale on the Dark Web. Finally, *Fero* raises questions about whether reliance on extrinsic evidence is—or should be—an approach courts adopt in addressing standing at the motion to dismiss stage where the evidentiary record is incomplete, and whether forensic reports and investigations prepared in the wake of data breaches may increasingly be subject to discovery. Whether the use of Dark Web searches and reliance upon forensic reports at the pleading stage becomes more common remains to be seen, but the case is one to watch.

BY ANDREW B. SERWIN, PURVI G. PATEL, AND ALEXANDRA LAKS

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com