The Dark Web and Other Mysteries

The web is bad enough, when it comes to invasion of privacy, but the Dark Web is something else altogether. In the unique case of *Clemens vs. ExecuPharm Inc.,* 2022 U.S. App. LEXIS 24808 (September 2, 2022) (Greenaway, Jr., C.J.), the United States Court of Appeals for the Third Circuit had the opportunity of looking at the harm caused to a company employee when her privacy was invaded by the ominous Dark Web.

Jennifer Clemens asked the Third Circuit to reverse the District Court's dismissal of her Complaint seeking equitable and monetary relief in connection with a data breach. The breach resulted in the publication of her sensitive personal information on the Dark Web. What exactly the Dark Web is, is a horse of a different color, or should we say a horse with a different web?

Clemens had argued that her injury was sufficiently imminent to constitute an injury-in-fact for purposes of standing. Standing seems to be all the rage these days. Back in the 70's, standing was a preeminent doctrine, giving rise to many law school articles. Lots of young lawyers toiled through the night trying to figure out what standing was. In fact, it is frequently a convenient tool to toss out a case. Ultimately, standing is based upon the "case and controversy" requirement found in the United States Constitution. United States courts do not issue Advisory Opinions. This has given rise to the "standing" industry.

Here, the appellant prevailed. The Third Circuit vacated the judgment of the District Court and remanded for consideration of the merits.

Clemens was a former employee of ExecuPharm Inc. She was required to provide her employer with sensitive personal and financial information. This included her address, social security number and other such items, many of which probably had little or no relevance to her employment.

ExecuPharm **promised** to protect the confidentiality of their employees. They assured Clemens that her information would be secure with ExecuPharm. Perhaps it was just a matter of *schlecht mazel*, bad luck, but after Clemens left ExecuPharm, the company was hacked and her information was stolen.

Fortunately, Clemens was a sharp tool in the woodshed and she took immediate action to mitigate the harm. Among other things, Clemens sued ExecuPharm and its parent, seeking to represent herself and others under the Class Action Fairness Act.

This brings us back to the insufferable, but often relied upon garbage can concept of "standing." The court discussed that the injury in this case, the so-called injury-in-fact, was "concrete."

> We hold that in the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, plaintiff suing for damage can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms.

The Court provided examples for the literate and illiterate alike. If the plaintiff's knowledge of the substantial risk of identity theft causes the plaintiff to experience emotional distress or spend money on mitigation measures, the plaintiff has sufficiently alleged a concrete injury. What are mitigation measures? Engaging a credit monitoring service would be one of them. Clemens did allege a substantial risk of harm could occur, and this seemed to be reinforced by the fact that the Dark Web was the culprit.

Clemens further alleged facts that established so-called traceability, at least at the pleading stage. She identified injuries which the former employee suffered as a direct and proximate result of the breach of contract. The failure to safeguard her information by her former employer, permitted Clemens' private data to be published on the Dark Web. One wonders whether the result would have been the same had the employee's information been published on the good old, typical, obnoxious, intrusive regular web.

The Circuit Court vacated the District Court's dismissal regarding the claims and remanded for consideration on the merits.

Also alleged was a tort action. Clemens had sufficiently alleged standing to bring a tort action as well. The District Court's dismissal of the tort claim was also vacated.

Imminence seemed to be very important to the Court as well.

> Because we have rejected the contention that risk of identity theft or fraud cannot qualify as sufficiently imminent, and hold that Clemens has alleged an injury-in-fact, we likewise vacate the District Court's decision and remand for determination of the merits of these claims.

Clemens was said to have to assert a contract, tort and secondary contract claims. Clemens properly alleged a future injury. What was that? The risk of identity theft or fraud was not only imminent, but further negative consequences could flow in the future as it would be obvious to even the most naïve user of the web.

The breach occurred as a result of a well-known hacking group, Clop. This awful sounding organization, and it's probably worse in reality than it sounds, intentionally stole the information, held it for ransom and published to the Dark Web. This made Clemens' sensitive data accessible to criminals worldwide.

Once upon a time, our office suffered a ransomware attack. Fortunately, I do crazy things like work Sunday nights, and I noticed something was amiss. Our very capable, competent tech person, Amber, came to the office the next morning and discovered the demand for ransom. She shut the system down, thus losing probably a half day worth of work. We notified the FBI and told the intruders to "go to hell." Fortunately, we did not pay a dime, but the episode was a rude awakening for us. Most professionals have little or no knowledge of what goes on in the web, let alone the Dark Web. The threat which we all face is titanic, and nobody wants to go to the bottom of the sea as a result of criminals invading our database.

In the Clemens situation, the nature of the information, personal and financial data, was certainly the type that could be utilized to perpetrate identity theft or fraud. Intangible items like publication of personal information, wrote the Court, does qualify as concrete. A plaintiff cannot be forced to wait until the threat and harm has occurred. Merely the theft of the data by really bad people provides sufficient potential harm so that the former employee has suffered an injury-in-fact and therefore has standing. Whether the imminent risk of identity theft is really a standing question, is an interesting issue, potentially a quagmire at best.

Whether the risk to the former employee created standing is almost beside the point. What is important is that there was a contractual duty on the part of the employer to safeguard the employee's information. For whatever reason, the employer was not able to do that, the information was stolen and the former employee is now at risk. There is a component of this case which is almost strict liability. It does not appear that sloppiness, neglect or fraud will be necessary on the part of the employer for plaintiff to prevail in her case.

Not too long ago, I had a client who settled a case with a lawyer in another state. The account of the client was hacked and the hacker directed the lawyer to send the settlement money to the hacker's account in Hong Kong. In spite of the lawyer having some knowledge that his client wanted the money sent to an institution in the U.S., the attorney nevertheless sent the money to Hong Kong. Needless to say, the money is gone and the lawyer is now a defendant in a federal action. A word to the wise is sufficient: carry insurance, which the lawyer did not, and have a robust system for handling your client's money.

While *Clemens vs. ExecuPharm*, did not involve law firms, financial institutions such as banks, and especially attorneys, are very much at risk from invaders roaming the regular web and the Dark Web. As my Dad used to say: "A word to the wise is sufficient."

The take away bullet points are as follows:

- Plaintiff Clemens was an ex-employee of a company to whom she had to give all of her confidential information.
- The company promised it would protect that information.
- A hacker got into the information and published it on the Dark Web.
- Clemens had standing to assert her contract tort and secondary contract claims.
- In return for her work and promises, the company had promised to safeguard the information, which it did not.
- She has alleged a future injury as well, risk of identity theft or fraud that is sufficiently imminent.
- The breach was conducted by a known hacking group.
- Dismissal by district court is reversed.

While standing enabled this plaintiff to prevail, it seems that the courts are going to take data breaches of employees' sensitive information and others as a very serious matter.

Clifford A. Rieders, Esquire
Rieders, Travis, Dohrmann, Mowrey
Humphrey & Waters
161 West Third Street
Williamsport, PA 17701
(570) 323-8711 (telephone)
(570) 323-4192 (facsimile)

Cliff Rieders is a Board-Certified Trial Advocate in Williamsport, is Past President of the Pennsylvania Trial Lawyers Association and a past member of the Pennsylvania Patient Safety Authority. None of the opinions expressed necessarily represent the views of these organizations.