Cybersecurity Risks: New Developments Regarding Employer Liability For Work-Related Identity Theft

November 2022

By: Thomas Reilly

Porzio Employment Law Monthly

Even before the age of remote work, most employers maintained internal servers hosting a plethora of sensitive information. Then, as now, employers typically go to great lengths to protect their sensitive internal and proprietary information from data breaches. But employers may think less about their employees' sensitive information, which may be hosted on their servers and which hackers may use after obtaining that information through a data breach.

In a recent federal case, *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 157–58 (3d Cir. 2022), the Third Circuit Court of Appeals held that an employee had standing to bring negligence and breach of contract claims against her employer after her personal information was published on the dark web due to a data breach. The employer, a global pharmaceutical subsidiary known as ExecuPharm, required the plaintiff to provide sensitive personal and financial information, including information regarding her financial accounts and her social security number, and promised to take "appropriate measures" to protect this information after it was stored on its servers.

After the plaintiff ended her employment with ExecuPharm, a hacking group accessed ExecuPharm's servers through a phishing attack and stole sensitive information pertaining to current and former employees, including the plaintiff. The group later posted this information on underground websites on the dark web, a hidden and difficult to access portion of the internet that serves as a black market for illegal products such as stolen data and personal information. ExecuPharm alerted its current and former employees of the breach and advised them to take appropriate precautionary measures. The plaintiff took several such protective measures. The measures apparently worked; the plaintiff's personal information was never used by any unauthorized person.

However, despite the lack of any actual theft or other harm suffered by the plaintiff, the plaintiff sued in federal court, alleging negligence and breach of contract against ExecuPharm. ExecuPharm moved to dismiss, arguing that the plaintiff did not have standing to sue because she suffered no actual harm. The Federal District Court dismissed the matter, and the plaintiff then appealed to the Third Circuit Court of Appeals. After reviewing the case law, the Third Circuit reversed and reinstated the plaintiff's claims. The Court explained that the data breach and resulting disclosure of the plaintiff's personal and financial data created a "substantial risk that the harm will occur sufficient to establish an 'imminent' injury." Moreover, the "disclosure of private information" alone constituted a cognizable harm, as did the emotional and other

distress that the plaintiff suffered because of the information leak. See 48 F.4th at 157–58. In summarizing its holding, the Court stated that employers must remain diligent and maintain sufficient security standards to protect their employees' private information. The Court stated:

In an increasingly digitalized world, an employer's duty to protect its employees' sensitive information has significantly broadened. Information security is no longer a matter of keeping a small universe of sensitive, hard-copy paperwork under lock and key. Now, employers maintain massive datasets on digital networks. In order to protect the data, they must implement appropriate security measures and ensure that those measures continue to comply with ever-changing industry standards.

[*Id*. at 158.]

The Court's holding presents a clear warning to employers, who may be liable to their employees for security and data breaches ***even if*** the employees suffer no actual financial harm. The decision creates a new layer of complexity for employers dealing with cybersecurity threats, who now face potential liability to their current and former employees in addition to the other numerous negative consequences that may flow from a data breach. Going forward, employers must ensure that they maintain appropriate and up-to-date security measures to provide strong and broad protection for the sensitive information stored on their servers and understand that a data breach may expose them to employee lawsuits.