



Kentucky Federal District Court Allows Claims in W-2 Data Breach Class Action to Proceed

Dec 12, 2017

Categories:
[Publications](#)

Authors:
[Michael E. Nitardy](#)

The fallout from the seemingly endless W-2 phishing scams continues to be felt. On December 1, 2017, a federal court in Louisville, Kentucky, in *Savidge v. Pharm-Save, Inc.*, 2017 WL 5986972, *1 (W.D.Ky. Dec. 1, 2017) determined that former employees could proceed with certain claims against their former employer arising from the improper disclosure of W-2's as a result of a phishing scam suffered by the employer.

The underlying facts of the *Savidge* case involve a 2016 phishing email scheme that resulted in defendant Pharm-Save, Inc. (and, as alleged in the Complaint under alter-ego theories, co-defendant Neil Medical Group, Inc.) disclosing employee W-2s to the criminal perpetrators. The plaintiffs are former employees who filed suit in a class action against Defendants on behalf of all current and former employees who were impacted by the breach.

The Complaint included counts for negligence, negligence per se, breach of implied contract, breach of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress. The Defendants moved to dismiss the complaint as to all counts, but the Court agreed to permit the case to proceed on two of the claims. In doing so, it provided insight into how courts may analyze such data breach cases.

The Negligence Claim

For the "duty" and "breach" elements of a negligence claim, while the Court admitted the allegations in the Complaint were "scant," the Court accepted that a reasonable inference that, because Plaintiffs' information was released to unauthorized individuals, Defendants breached their duties to safeguard that information.

While a number of data breach cases have failed on the damages element due to the speculative nature in which damages in this area

have been pled, the Court in *Savidge* found sufficient pleading of damages to maintain the negligence action – though it noted that the mere attempted filing of a fraudulent tax return in one of the Plaintiffs’ name alone was not enough to cause cognizable injury.

Instead, the Court found persuasive the Plaintiffs’ allegations of damages from out-of-pocket expenses incurred and lost productivity time spent in monitoring activity to prevent and address possible fraudulent tax returns, damages which other courts have deemed too speculative to withstand a motion to dismiss.

The Court relied upon a growing number of federal district and appellate courts that have recognized as “injury-in-fact” the expense incurred in purchasing credit monitoring services and the costs expended to deal with fraudulent activity following the theft of PII, particularly where such stolen PII has already been used by the perpetrators. For example, the Court found the perpetrators’ attempted filing of a tax return for Plaintiff Savidge compelling on this point.

In addition, the Court found a sufficient “nexus” between the data breach and the alleged fraudulent activity to satisfy the “causation” element. In so finding, the Court relied on the fact that the Defendant itself warned its employees and former employees of possible attempts by the criminals to file fraudulent tax returns. The Court stated that because that was precisely what happened in Plaintiff Savidge’s case, a sufficient nexus had been established.

Breach of Implied Contract Claim

The Court had no problem finding an implied promise by the Defendant to keep confidential the personal information of the Plaintiffs necessary to create the W-2 forms, and a breach of that promise by their unauthorized release of that information to the perpetrators. It cited the involuntary nature of the requirement that employees provide employers with their sensitive information, such as Social Security numbers, and that that requirement gave rise to an implied agreement by the Defendants to protect the Plaintiffs’ information.

Takeaways

Although the two claims that survived Defendants' Motion to Dismiss are based on different legal theories, they both are based on an employer's obligation to protect employees' personal information.

As a result, *Savidge* continues the movement of courts towards finding that if sensitive employee personal information is disclosed to third-parties without the employee's consent, it is not unreasonable to assert at the pleading stage that such disclosure was the result of a breach of an employer's duty or an employer's promise. This has consequences not only for employers, but also for all individuals and entities that use or control personal information. Given the ever-increasing number of breaches and scams, and the increasing likelihood for organizations that a breach is not a matter of "if" but "when," being able to demonstrate that the breach or scam was not the result of any duty or promise that was breached by the organization becomes incredibly important. Potential ways to demonstrate that no duty was breached include providing regular training of employees on potential phishing threats and maintaining an up-to-date IT system. Failure to perform these tasks may make organizations vulnerable to class action suits should they find themselves victimized by hackers and scammers.

In addition, *Savidge* also supports the concept that pleading additional out-of-pocket costs incurred with the reasonable threat of harm as a result of the breach or disclosure will meet a plaintiff's requirement to sufficiently plead damages in a data breach case. Given that many companies currently provide credit monitoring of some type for at least a year after a data breach, companies may rightly wonder if such a provision will be enough to ward off future claims for damages.

For more information, contact [Michael Nitardy](#), or any other member of Frost Brown Todd's [Privacy & Data Security Team](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.