Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 5 / AUGUST 14, 2015

EXPERT ANALYSIS

Efficacy of FCRA Claims Based on Stolen Data In Data Breach Cases

By John J. Delionado, Esq., and Jason M. Beach, Esq.
Hunton & Williams

Plaintiffs often must shoehorn new and evolving factual scenarios into older laws. Data breach litigation is a quickly developing area, and the federal Fair Credit Reporting Act[1] is an older law.

Many people consider the FCRA, enacted in 1970, to be the nation's first privacy law. It was designed to formalize the way the consumer reporting industry had functioned for many years. The FCRA identifies the responsibilities of agencies that create and distribute consumer reports and consumers' rights regarding those reports.

The FCRA contains disclosure obligations for reporting agencies and the users of relevant reports to inform consumers when their reports have been used as a basis for an adverse decision against them. In some cases, these disclosures alert consumers about fraudulent use of their credit accounts or other errors in their credit files that may be the result of faulty reporting or identity theft.[2]

The FCRA's statement of purpose generally calls for "reasonable procedures" designed for the "confidentiality, accuracy, relevancy and proper utilization" of consumer information.[3] To that end, the FCRA details how consumer reporting agencies must assemble and evaluate consumer credit information and other personal details, and how they must provide this information to third parties.

As a strategic matter, the FCRA was an attractive statute for data breach plaintiffs to invoke for subject matter jurisdiction in federal court. A number of data breach causes of action are anchored in state law, including claims for negligence, breach of implied contract, invasion of privacy and unjust enrichment.

For FCRA claims in data breach cases, plaintiffs whose information was stolen or otherwise exposed frequently allege the hacked companies improperly transferred their consumer information to unauthorized third parties. Because the FCRA targets only certain types of entities, some defendants respond that they are not subject to the federal law, arguing they are not "consumer reporting agencies."[4]

Defendants usually challenge standing as well. In fact, the U.S. Supreme Court has decided to review a standing issue under the FCRA in the upcoming term, in *Spokeo Inc. v. Robins*.[5] The Supreme Court's ruling in the case may significantly affect future standing considerations in data-breach-focused FCRA actions, especially where damages or injuries may be difficult to establish.

However, companies that face FCRA claims when data is stolen through a breach or hack have another — simpler — defense: The failure to safeguard stolen data does not qualify as "furnishing consumer reports" under the FCRA.

To illustrate, a case against Countrywide Financial Corp. involved the theft of millions of customers' sensitive personal and financial information. The court found that "[t]he applicable provisions of the FCRA extend liability only where consumer reports are 'furnished' or disseminated in a manner that violates the FCRA."[6]

Noting that the FCRA did not define "furnish," the court held that common sense underscored why Countrywide was not liable under the FCRA: "No coherent understanding of the words 'furnished' or 'transmitted' would implicate Countrywide's action." Instead, a perpetrator independently stole Countrywide's customer information to illegally sell it, the court noted.

Subsequent cases have agreed.

One proposed class action targeted a payment processor after a data breach in 2012. The stolen information included data that could be used to counterfeit new cards. Potentially 1.5 million customers' information was compromised, and the payment processor found itself defending, among other causes of action, an FCRA claim.

In dismissing the FCRA claim, the court emphasized that the data was *stolen*, not furnished. The court reasoned that the term "furnish" involves the act of "transmit[ting] information" to another, which is difficult to reconcile with the failure to safeguard stolen data.[7]

The court in *In re Sony Gaming Networks & Customer Data Security Breach Litigation* also dismissed FCRA claims, without allowing the plaintiffs to amend their complaint on this issue, because Sony never "furnished" the stolen data, as required under the FCRA.[8]

Other federal cases similarly demonstrate that the "stolen" distinction can be a critical fact.[9]

Additionally, a dismissal under Federal Rule of Civil Procedure 12 may not be worst outcome for attorneys bringing FCRA claims premised on stolen data.

As a strategic matter, the FCRA was an attractive statute for data breach plaintiffs to invoke for subject matter jurisdiction in federal court.

At least one case has signaled that overreaching FCRA allegations may warrant sanctions under Federal Rule of Civil Procedure 11.[10] The issue arose in a proposed class action arising from a cyberattack on the South Carolina Department of Revenue, which exposed about "3.6 million Social Security numbers, 387,000 credit and debit card numbers and tax records for 657,000 businesses."[11] The defendant was Trustwave Holdings Inc., a Chicago-based data security company that the Department of Revenue had hired to protect its data.

In dismissing the FCRA claim, the court reasoned the allegations did not state Trustwave had some side business to distribute consumer reports. Instead, the plaintiff argued that Trustwave was a consumer reporting agency because it "assembled" consumer data by virtue of the data security services it provided. The plaintiff also contended that Trustwave "furnished" that data as a result of its negligent or willful failure to safeguard the data.

The court found it significant that the plaintiff did not allege, and could not plausibly maintain, that Trustwave's "purpose" was to furnish the information to data thieves. Rather, the complaint alleged that Trustwave's purpose was just the opposite: to prevent anyone from getting the information. Although the court allowed the plaintiff to replead the FCRA claim, it warned the plaintiff's attorneys that the FCRA claim, as asserted, raised serious Rule 11 concerns.

CONCLUSION

In sum, "[a]lthough 'furnish' is not defined in the FCRA, courts generally use the term to describe the active transmission of information to a third party rather than a failure to safeguard the data."[12] With Article III standing issues for FCRA claims currently in flux, this simple, commonsense argument can be an effective way to pursue dismissal in data breach cases.

The increase in reported cases addressing FCRA claims after a data breach, along with the threat of Rule 11 sanctions for some of the more creative applications in this context, may signal a decrease in the number of FCRA claims based on stolen data in future breach cases.

NOTES

[1] 15 U.S.C. § 1681.

[2] Lisa J. Sotto, Privacy and Data Security Law Deskbook § 2.01 (2014). The FCRA was amended in 2003 to protect consumers from the growing threat of identity theft.

[3] 15 U.S.C. § 1681(b).

[4] The FCRA places distinct obligations on three types of entities: consumer reporting agencies, users of consumer reports and furnishers of information to consumer reporting agencies. *Chipka v. Bank of Am.,* 355 F. App'x 380, 382 (11th Cir. 2009). Most of the FCRA's requirements, however, generally extend to consumer reporting agencies. "The term 'consumer reporting agency' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). Members of the health care, retail and financial services industries who merely pass along information concerning certain debts that are owed to them, or for certain verification purposes, generally are not considered credit reporting agencies. *Falkenberg v. Alere Home Monitoring Inc.,* No. 13-CV-00341, 2015 WL 800378, at *5 (N.D. Cal. Feb. 23, 2015); *Tierney v. Advocate Health & Hosps. Corp.,* No. 13 CV 6237, 2014 WL 5783333, at *3 (N.D. Ill., E. Div. Sept. 4, 2014); *Mirfasihi v. Fleet Mortg. Corp.,* 551 F.3d 682, 686 (7th Cir. 2008); *DiGianni v. Stern's,* 26 F.3d 346, 348 (2d Cir. 1994).

[5] No. 13-1339 (U.S. Apr. 27, 2015). Spokeo.com provides information about an individual, including "contact data, marital status, age, occupation, economic health and wealth level." *Robins v. Spokeo Inc.,* 742 F.3d 409, 410 (9th Cir. 2014), *cert. granted,* 135 S. Ct. 1892 (2015). The plaintiff claimed that Spokeo harmed his employment prospects by reporting he was employed and holding a graduate degree (both of which were untrue) as well as by overstating his wealth. He sued for statutory damages under the FCRA. Although Spokeo asserted that it was not a credit reporting agency, the issue addressed by the 9th Circuit, and now certified by the Supreme Court, is whether violations of statutory rights created by Congress alone are sufficient to satisfy Article III standing. The 9th Circuit reversed the trial court's dismissal order and held that allegations of statutory right violations were sufficient to establish the injury-in-fact prong of Article III standing.

[6] *Holmes v. Countrywide Fin. Corp.,* No. 5:08-CV-00205, 2012 WL 2873892, at *15 (W.D. Ky., Paducah Div. July 12, 2012).

[7] *Willingham v. Global Payments Inc.,* No. 1:12-CV-01157, 2013 WL 440702, at *13 (N.D. Ga., Atlanta Div. Feb. 5, 2013).

[8] 996 F. Supp. 2d 942, 1012 (S.D. Cal. 2014).

[9] *Tierney*, 2014 WL 5783333, at *3 (dismissing FCRA claim when "[p]laintiffs fail to plausibly allege that defendant 'furnished' any information to a third party; rather, plaintiffs allege that computers containing personal information were stolen"). *See also Burton v. MAPCO Exp. Inc.,* 47 F. Supp. 3d 1279, 1287 (N.D. Ala., N.E. Div. 2014) (dismissing FCRA claims in proposed class action when, among other reasons, plaintiffs failed to support that "the theft of credit card information constitutes 'furnishing consumer reports'").

[10] Fed. R. Civ. P. 11(b)(2). Rule 11 requires claims to be "warranted by existing law or by a nonfrivolous argument" that the law should be changed.

[11] *Strautins v. Trustwave Holdings Inc.,* 27 F. Supp. 3d 871 (N.D. Ill., E. Div. 2014).

[12] *Dolmage v. Combined Ins. Co. of Am.,* No. 14 C 3809, 2015 WL 292947, at *3 (N.D. Ill., E. Div. Jan. 21, 2015) (dismissing FCRA claims in proposed class action arising from a data breach).

John J. Delionado (L) is a partner with **Hunton & Williams** based in the Miami and Washington offices. His practice focuses on internal investigations, financial institution defense and cybersecurity matters. He can be reached at jdelionado@hunton.com. **Jason M. Beach** (R) is a counsel based in Hunton's Atlanta office whose practice focuses on complex commercial litigation, cybersecurity/data breach issues and government regulatory matters. He can be reached at jbeach@hunton.com. This article presents the views of the authors and does not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.

Companies facing FCRA claims when data is stolen through a breach or hack have another — simpler — defense: The failure to safeguard stolen data does not qualify as "furnishing consumer reports" under the FCRA.

This article presents the views of the authors and do not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.