Federal Court Dismisses Data Breach Class Action Brought Against J.P. Morgan Chase Based on Federal Preemption

ALAN CHARLES RAUL, EDWARD McNICHOLAS, MICHAEL F. McENENEY, AND KARL F. KAUFMANN

This article discusses a recent New York district court case holding that the Fair Credit Reporting Act ("FCRA") requirements for data disposal will preempt similar state laws, thereby making it more clear that financial institutions may be able to rely upon the federal data disposal requirements for credit report information without regard to the growing number of state data disposal laws.

A federal district court in New York has dismissed a putative class action against J.P. Morgan Chase, N.A. ("Chase") by plaintiffs seeking relief under federal and New York state laws for damages allegedly suffered following a massive loss of customer credit card data.[1] The court rejected the plaintiffs' federal claims for failing to allege actual damages, and ruled that the plaintiffs' state law claims were preempted by federal law. Significantly, the court's decision provides the first judicial interpretation of "conduct" relating to data disposal where FCRA requirements will preempt similar state laws. More specifically, the court interpreted 15 U.S.C. § 1681t(b)(5)(I) to preclude any state attempt to regulate

Alan Charles Raul, Edward R. McNicholas, Michael F. McEneney, and Karl F. Kaufmann are partners in the Washington D.C. office of Sidley Austin LLP. They may be contacted at araul@sidley.com, emcnicholas@sidley.com, mmceneney@sidley.com, and kkaufmann@sidley.com, respectively.

Published in the October 2009 issue of Privacy & Data Security Law Journal.
Copyright ALEXeSOLUTIONS, INC.
1-800-572-2797

behavior governed by the FCRA or federal regulations issued pursuant to the FCRA.

The suit followed a September 2006 announcement by Chase that it had unintentionally discarded several computer tapes containing the personal information of 2.6 million credit card holders. On February 17, 2009, James Willey filed a class action complaint on behalf of himself and all persons affected by the data loss, claiming that Chase violated the FCRA and several state claims. Chase filed a successful motion to dismiss the complaint in its entirety under Fed. R. Civ.P. 12(b)(6) for failure to state a claim.

PLAINTIFF'S FCRA CLAIMS FAIL TO MEET PLEADING STANDARDS AND ARE DISMISSED WITH PREJUDICE

The court first addressed the plaintiffs' claims under the FCRA, which governs the disposal of consumer information.[2] The FCRA requires agencies, including the Office of the Comptroller of the Currency ("OCC"), to issue regulations regarding the disposal of consumer information derived from consumer reports.[3] The OCC's regulation requires that banks "properly dispose of any consumer information it maintains or otherwise possesses"[4] in accordance with the Interagency Guidelines Establishing Information Security Standards ("Interagency Guidelines").[5] The Interagency Guidelines require banks to "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities" and require that a bank's board of directors "approve and oversee the development and implementation" of the program.[6] The programs must be able to identify foreseeable threats, assess the threats' potential impact, and determine the adequacy of existing measures to control threats.[7] The FCRA may be enforced through a private right of action for willful or negligent violations of duties imposed by the statute, allowing recovery of actual damages for negligent violations and actual, statutory, and punitive damages for willful violations.[8] The plaintiffs' suit alleged both willful and negligent violations of the FCRA.

Published in the October 2009 issue of Privacy & Data Security Law Journal.
Copyright ALEXeSOLUTIONS, INC.
1-800-572-2797

The court found that the plaintiffs' claims fell "well short" of federal pleading standards, consisting only of "formulaic" recitations of the elements of a cause of action under the FCRA with no supporting factual allegations.[9] The court, relying upon *Bell Atlantic Corp*. v. *Twombly*[10] and *Ashcroft* v. *Iqbal*,[11] found these pleadings insufficient to allow the suit to proceed to discovery, noting that the Supreme Court in *Iqbal* recently rejected the idea that plaintiffs can subject defendants to discovery with merely conclusory pleadings.[12]

The court dismissed the plaintiffs' claims with prejudice because the FCRA statute of limitations — which in this case extended for only two years following the plaintiffs' awareness of the putative violation — barred the filing of an amended complaint.[13] Chase argued that Willey and other potential plaintiffs became, or should have become, aware of the data loss following the Chase announcement and its widespread coverage in national media. The court agreed, noting that the publicity surrounding the data disposal contained highly detailed and specific information and was sufficient to put plaintiffs on notice.[14]

STATE CLAIMS ARE PREEMPTED BY THE FCRA AND FAIL TO STATE ACTUAL DAMAGES

The court dismissed the plaintiffs' state law claims as "repetition[s]" of the FCRA claims, finding that Congress intended the FCRA to preempt state laws attempting to regulate conduct subject to FCRA provisions.[15] The FCRA contains a preemption provision stating "[n]o requirement or prohibition may be imposed under the laws of any state…with respect to the conduct required by the specific provisions of…section 1681w of this title."[16] FCRA Section 1681w requires federal banking agencies to promulgate regulations requiring proper data disposal by banks; the OCC issued the regulations at issue in *Willey* under Section 1681w. The court noted that the question of how to interpret the FCRA preemption provision concerning "conduct required" by OCC programs was of first impression before a federal court.[17] While the plaintiffs argued for a narrow construction of "conduct," the court instead adopted the broad meaning Chase

Published in the October 2009 issue of Privacy & Data Security Law Journal.
Copyright ALEXeSOLUTIONS, INC.
1-800-572-2797

suggested, holding that the "conduct" in question refers to all conduct falling within the scope of OCC regulations.[18] By establishing a broad interpretation of conduct governed exclusively by the FCRA in 15 U.S.C. 1681t(b)(5)(I), the court's decision, if adopted elsewhere, may effectively preclude numerous state law claims following allegedly improper data disposal covered by OCC and other banking agency data security regulations. Since FCRA Section 1681w required that the National Credit Union Administration, the Federal Trade Commission, and the Securities and Exchange Commission all promulgate data disposal guidelines, the court's interpretation of FCRA preemption could be extended to apply to the conduct of a broad variety of entities other than banks.[19]

The court also found the plaintiffs' state law claims deficient insofar as they failed to allege actual damages, a required element for each claim. While noting that emotional damages may suffice for claims under the FCRA, the court held that "[i]n state information loss cases…[t]he risk that plaintiff's data *may* be misused because it has been lost is not a cognizable harm."[20] The court declined to consider the costs of protecting against identity theft as a form of damages, and dismissed the plaintiffs' state law claims on these grounds as well.

IMPLICATIONS OF THE *WILLEY* RULING

The *Willey* court may provide a framework for a successful defense to state law claims arising from allegedly improper data disposal. By demonstrating how the language in FCRA Sections 1681t and 1681w preempts state regulation of any conduct governed by federal regulations issued pursuant to the FCRA, the court seriously undercuts the possibility of filing state law claims in conjunction with citizen suits under the FCRA. Of course, it is uncertain how widely other courts will adopt this view, even with similar fact patterns.

The *Willey* court also continues a trend of federal courts dismissing suits claiming only potential, or speculative, injuries from data breaches or losses — rather than any actual identity theft. The court cited *Pisciotta* v. *Old Nat'l Bancorp*[21] and *Caudle* v. *Towers, Perrin, Forster & Crosby*, Inc.[22] to illustrate this point. Reliance upon these two cases, however, sug-

Published in the October 2009 issue of Privacy & Data Security Law Journal.
Copyright ALEXeSOLUTIONS, INC.
1-800-572-2797

gests that the court was willing to take the plaintiffs' Article III standing as a given, even as it dismissed their claims for failure to allege damages. Unlike the many courts[23] that have dismissed suits for plaintiffs' failure to allege injury sufficient to confer standing, the Seventh Circuit in *Pisciotta* found that "[t]he injury-in-fact requirement can be satisfied by a threat of future harm or by an act which increase[es] the risk of future harm" to the plaintiff.[24] The *Caudle* court agreed with this rationale, citing to *Pisciotta* and environmental damages cases in support.[25] Although the *Willey* ruling may suggest that courts are willing to follow *Pisciotta* and recognize standing in data breach cases, the outcome reveals that the absence of actual harm to plaintiffs will likely continue to preclude them from eventual legal victory.

NOTES

[1] *Willey* v. *J.P. Morgan Chase, N.A.*, No. 09 Civ. 01397 (CM) (S.D.N.Y. July 7, 2009).

[2] The relevant FCRA provisions are found at 15 U.S.C. §§ 1681w. Banks such as Chase are subject to FCRA governance under the authority of the Office of the Comptroller of the Currency ("OCC"), which details its requirements for FCRA compliance at 12 C.F.R. § 41 and pt. 30, App. B ("Interagency Guidelines Establishing Information Security Standards").

[3] 15 U.S.C. 1681w(a)(1).

[4] 12 C.F.R. § 41.83.

[5] 12 C.F.R. pt. 30, App. B.

[6] *Willey*, at 6 (citing 12 C.F.R. pt. 30, App. B, II(A)).

[7] 12 C.F.R. pt. 30, App. B, III(B)(1-3).

[8] 15 U.S.C. §§ 1681n, 1681o.

[9] *Willey* at 7-8.

[10] 550 U.S. 544, 555 (2007).

[11] 129 S.Ct. 1937, 1951 (2009).

[12] *Willey* at 7-8.

[13] *Id.* at 12.

[14] *Id.*

[15] *Id*. at 13.

[16] 15 U.S.C. § 1681t(b)(5)(I).

Published in the October 2009 issue of Privacy & Data Security Law Journal.
Copyright ALEXeSOLUTIONS, INC.
1-800-572-2797

[17] *Willey* at 14.
[18] *Id*. at 14-17.
[19] 15 U.S.C. § 1681w(a)(1).
[20] *Id*. at 18.
[21] 499 F.3d 629 (7th Cir. 2007).
[22] 580 F. Supp. 2d 273 (S.D.N.Y. 2008).
[23] *See, e.g., Randolph* v. *ING Life Ins. and Annuity Co*., 486 F. Supp. 2d 1, 8-9 (D.D.C. 2007); Bell v. Acxiom Corp., No. 4:06 Civ. 00485, 2006 U.S. Dist. LEXIS 72477, at *8-10 (E.D.Ark. Oct. 3, 2006); *Giordano* v. *Wachovia Sec., LLC*, No. 06 Civ. 476, 2006 WL 2177036, at *5 (D. N.J. July 31, 2006).
[24] *Pisciotta,* 499 F.3d at 634.
[25] *Caudle*, 580 F. Supp. 2d at 280.

Published in the October 2009 issue of Privacy & Data Security Law Journal.
Copyright ALEXeSOLUTIONS, INC.
1-800-572-2797