

WSGR ALERT

JANUARY 2011

NINTH CIRCUIT HOLDS THAT INCREASED RISK OF IDENTITY THEFT IS SUFFICIENT FOR ARTICLE III STANDING: *PRIVACY CLASS ACTIONS LIKELY TOUGHER TO DISMISS*

The U.S. Court of Appeals for the Ninth Circuit held recently, in *Krottner v. Starbucks Corporation*,¹ that increased risk of future misuse of personal data following the theft of a laptop containing the unencrypted personal data of a group of current and former Starbucks employees amounted to an injury sufficient to confer standing to sue in federal court. Despite concluding that standing existed under Article III of the Constitution, the Ninth Circuit nonetheless upheld the dismissal of plaintiffs' claims because they failed to allege an injury sufficient to state a claim under the relevant state law.

While the decision is limited to the very narrow facts contained in the record, it highlights the challenges defendants face in defeating class actions arising out of data breach incidents at the pleading stage, even when there has been no alleged use of the data following the breach. A motion to dismiss for lack of standing due to no actual or imminent injury represents one of the most common defense tactics in this type of litigation. Such motions are filed prior to discovery and therefore have important economic advantages for defendants.²

The decision also highlights the risks of potential data-breach-related litigation faced by all companies that collect, maintain, and use personal data. It further illustrates the

increased importance of avoiding data breaches and developing effective response programs to manage related litigation risks when a breach occurs.

Background

The facts in *Krottner* resemble those of many common security breaches that have triggered notifications by companies. A laptop containing the unencrypted names, addresses, and Social Security numbers of approximately 97,000 Starbucks employees was stolen. Starbucks notified employees of the incident three weeks after the theft. In its notice, Starbucks encouraged the employees to monitor their financial accounts for financial activity and to take steps to protect themselves from identity theft. Starbucks also offered affected employees one free year of a credit-monitoring service.

Six months after the incident, two groups of employees filed class action lawsuits claiming that Starbucks had acted negligently and had breached an implied contract under Washington law. One plaintiff allegedly suffered from stress and anxiety regarding the situation. A second alleged that his bank had notified him that someone had attempted to open a new account using his Social Security number. The bank had closed the account, however, and the plaintiff did not allege that he suffered any financial loss. The second and a third plaintiff claimed, among

other things, that they had expended significant time and energy monitoring their financial accounts for identity theft, and faced an increased risk of future identity theft. The district court held that all three plaintiffs had standing to bring suit, but dismissed both complaints on the grounds that the plaintiffs had failed to allege a cognizable injury under Washington law. As a result, the district court held that the plaintiffs had failed to state a claim. The plaintiffs appealed to the Ninth Circuit.

Ninth Circuit Decision

To determine whether the plaintiffs had standing to bring suit under Article III of the Constitution, the Ninth Circuit applied the three-part test set forth by the U.S. Supreme Court in *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180-81 (2000). To have standing, a plaintiff must show that:

- (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.³

¹ *Krottner v. Starbucks Corp.*, Nos. 09-35823 and 35824 (9th Cir., Dec. 14, 2010).

² For examples of courts granting such motions, see *Amburgy v. Express Scripts, Inc.*, 671 F.Supp.2d 1046, 1051-52 (E.D. Mo. 2009); *Key v. DSW, Inc.*, 454 F.Supp.2d 684 (S.D. Ohio 2006).

³ *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167 (2000).

Continued on page 2...

Ninth Circuit Holds that Increased Risk of Identity Theft Is Sufficient for Standing . . .

Continued from page 1...

Because the latter two factors had not been disputed in the district court, the Ninth Circuit focused upon the first factor—whether the plaintiffs had suffered a sufficient “injury in fact.” The court held that the plaintiffs satisfied this requirement. One plaintiff satisfied the requirement by alleging generalized anxiety and stress as a result of the theft. The other two plaintiffs satisfied the requirement through their allegations of increased risk of future identify theft. In sum, the court concluded, the plaintiffs had “alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.”

By finding that the plaintiffs had standing, the Ninth Circuit joined the Seventh Circuit, the only other federal appellate court at the time of the decision that had specifically decided whether increased risk of future misuse of stolen personal data constituted an injury in fact for purposes of Article III standing.⁴ The court noted and rejected Sixth Circuit dicta questioning whether standing existed for risk of future identity theft since such risk was both “hypothetical” and “conjectural.”⁵ The *Krottner* court did not comment on numerous federal district courts’ opinions dismissing actions for lack of standing where the only injury alleged had been an increased risk of identity theft in connection with the compromise of personal data in a data breach incident.⁶

Even though the Ninth Circuit held that the plaintiffs had standing, it affirmed the district court’s dismissal of their two claims under Washington State law.⁷ First, the Ninth Circuit held that Washington law requires actual loss or damage, and not a “mere danger of future harm,” to support a negligence claim. The

injuries alleged by the plaintiffs all stemmed from future harm. The court also noted that the plaintiffs had waived any argument that a plaintiff’s alleged anxiety constitutes an actionable injury, as the plaintiffs had failed to raise it in their opening brief. Second, the court held that the plaintiffs, by failing to demonstrate any specific offer by Starbucks to protect their personal data—or to have accepted any such offer—had failed to plead the existence of an implied contract under Washington law.

The Ninth Circuit’s affirmation of the ultimate dismissal of the plaintiffs’ case remains consistent with the vast weight of authority addressing state law claims arising out of a data breach incident, which generally require actual damages to sustain the claim. As the *Pisciotta* court noted, plaintiffs continue to have a very difficult time alleging any type of legal theory upon which they can recover.⁸

Implications

Krottner is significant for its conclusion that data breach plaintiffs have standing to sue based only upon allegations of “generalized anxiety and stress” or an increased risk of identity theft as a result of the theft of a laptop containing personal data. Though the court dismissed the plaintiffs’ claims, the holding of standing likely will make it easier for class action lawsuits to proceed against companies that suffer data breach incidents in which personal information is compromised, even where the individuals whose data was compromised have not suffered any out-of-pocket damages. In particular, it seems likely that plaintiffs will look to assert statutory claims that do not require actual damages as an element.

Although courts’ unwillingness to grant relief to data breach plaintiffs who have not suffered cognizable damages has been welcomed by companies that have been victimized by such incidents, the costs of litigating these matters can be quite substantial. While all incidents cannot be avoided, many organizations can and do take steps to try to lower the frequency of such incidents. Moreover, when incidents do occur, responding quickly and effectively, with measures designed to help prevent misuse of the compromised personal data, can help manage related risks including class action litigation and government investigations.

In view of the risk for privacy- and data security-related litigation, companies may desire to understand the ongoing value of implementing appropriate data security measures to prevent personal information from unauthorized use and disclosure. Additionally, if a company suffers a security breach, a quick and effective response may help mitigate the potential consequences, and indeed may be required by numerous state and federal laws, such as those requiring notification in the event of a security breach.

Wilson Sonsini Goodrich & Rosati attorneys regularly assist clients with all aspects of their privacy and information governance needs, including efforts to prevent, mitigate, and respond to data breach incidents. If you have questions in these areas, please contact Tonia Klausner at tklausner@wsgr.com or (212) 497-7706; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; Matt Staples at mstaples@wsgr.com or (206) 883-2583; or another member of the firm’s privacy and data security practice (<http://www.wsgr.com/privacy>).

⁴ *Pisciotta v. Old National Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007).

⁵ See *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008).

⁶ See, e.g., *Randolph v. ING Life Ins. and Annuity Co.*, 486 F.Supp.2d 1, 6-8 (D.D.C. 2007) (no standing where laptop computer stolen during burglary and plaintiffs pled increased risk of identity theft); *Bell v. Acxiom Corp.*, No. 06-0485, 2006 WL 2850042, at *1-2 (E.D. Ark. Oct. 3, 2006) (class action dismissed for lack of standing where hacker downloaded information and sold it to marketing company); *Key v. DSW, Inc.*, 454 F.Supp.2d 684, 690 (S.D. Ohio 2006) (class action dismissed for lack of standing where unauthorized persons obtained access to information of approximately 96,000 customers, but no customers had suffered identity theft); *Giordano v. Wachovia Sec. LLC*, No. 06-476, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006) (credit monitoring costs resulting from lost financial information did not constitute injury sufficient to give plaintiff standing).

⁷ *Krottner v. Starbucks Corp.*, Nos. 09-35823 and 35824, slip op. at 1, 2 (9th Cir.; Dec. 14, 2010).

⁸ See *Pisciotta*, 499 F.3d at 634 (“Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy. Plaintiffs have not come forward with a single case or statute, from any jurisdiction, authorizing the kind of action they now ask this federal court . . . to recognize as a valid theory of recovery[.]”).

Continued on page 3...

Ninth Circuit Holds that Increased Risk of Identity Theft Is Sufficient for Standing . . .

Continued from page 2...



Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on January 24, 2011. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

This communication is provided for your information only and is not intended to constitute professional advice as to any particular situation. We would be pleased to provide you with specific advice about particular situations, if desired. Do not hesitate to contact us.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com

© 2011 Wilson Sonsini Goodrich & Rosati,
Professional Corporation
All rights reserved.