



Portfolio Media, Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Risks Of Sharing Employee Data With 3rd-Party Vendors

Law360, New York (August 09, 2012, 1:07 PM ET) -- A recently filed class action asserts claims against the Winn-Dixie supermarket chain and a third-party vendor, Purchasing Power LLC, in connection with the alleged theft of employee data provided to Purchasing Power in order to administer a discount purchasing program offered to Winn-Dixie employees. The claims advanced against Winn-Dixie and Purchasing Power highlight the potential risks associated with sharing employee or customer data with third-party vendors, and underscore the need for companies to ensure that the data security practices of third-party vendors are consistent with those of the companies themselves. The complaint also demonstrates how failure to make prompt disclosure of data breaches to affected individuals can increase the risk of class action litigation.

According to the complaint in *Burrows v. Purchasing Power LLC*, Case No. 1:12-cv-22800 (S.D. Fla.), Winn-Dixie either transferred or permitted Purchasing Power to access personally identifiable information of Winn-Dixie employees for the purpose of making a discount purchasing program available to Winn-Dixie's employees. The complaint alleges that Winn-Dixie notified employees on Jan. 27, 2012, that Winn-Dixie employee data had been inappropriately accessed by an employee of Purchasing Power. The notice further stated that Winn-Dixie first learned of the data theft in October 2011. According to the complaint, Winn-Dixie did not explain the reason for its delay in providing notice, and Purchasing Power has never, at any time, provided notice of the breach to Winn-Dixie employees.

One unique aspect of *Burrows* that distinguishes it from the typical privacy class action is an allegation that the named plaintiff suffered actual injury by reason of a data breach. Specifically, plaintiff alleges that the Internal Revenue Service refused to accept his 2011 federal income tax return, stating that a return had already been filed in his name. Plaintiff claims that someone who had access to the PII stolen from Purchasing Power filed the return, thereby depriving plaintiff of an anticipated refund. He seeks damages associated with the lost refund, in addition to other damages associated with the risk of further misuse of his PII.

The complaint asserts claims for negligence, violation of the federal Stored Communications Act, 18 U.S.C. § 2702, violation of the Florida Unfair and Deceptive Trade Practices Act, and breach of the common law right to privacy. Plaintiff asserts these claims on behalf of a putative class of all Florida employees of Winn-Dixie whose PII was provided to or accessed by Purchasing Power.

The complaint in *Burrows* has some evident flaws. The Stored Communications Act only applies to conduct by entities such as Internet service providers that are engaged in the "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). Neither the defendants nor the

conduct alleged facially meet this requirement. Further, the particularized harm allegedly suffered by the named plaintiff allows defendants to argue that determining whether class members suffered actual injury would raise highly individualized questions of fact that preclude certification of a plaintiff class to seek money damages under Fed. R. Civ. P. 23 (b)(3).

Nonetheless, certain aspects of *Burrows* pose challenges for the defendants. Where, as here, the data breach allegedly resulted from a targeted effort to steal PII — unlike cases involving thefts of laptops, in which any data theft is incidental — courts have been more receptive to claims that class members' costs to mitigate risk of identity theft constitute cognizable injury. The actual injury allegedly suffered by the named plaintiff supports the argument that the threat of misuse of the stolen data is not speculative and, therefore, warrants monetary and injunctive relief.

Burrows provides a timely reminder that it is critical that any company that shares customer or employee PII with a vendor must ensure that the vendor can adequately protect such data. Executing a written agreement specifying the company's and the vendor's respective data security obligations is a necessary, but not sufficient step. The contract will not be worth the paper on which it is written if the vendor lacks the capability to comply with its obligations.

Individuals responsible for the company's data security practices must engage in sufficient due diligence to assure the company that the vendor's data security practices are at least commensurate with the company's practices and otherwise comply with the legal requirements of all applicable states and jurisdictions. In addition, to provide proper incentives to adhere to contract requirements, the agreement should indemnify the company for any losses caused by the vendor's failure to satisfy its data security obligations.

Finally, *Burrows* illustrates the critical importance of prompt notification whenever a data breach occurs. If plaintiff was indeed victimized by someone who filed a bogus return using the plaintiff's stolen PII, notice to employees in October 2011, perhaps combined with proactive steps to protect affected employees from misuse of data, might have forestalled such an injury. Absent such an occurrence, it is unlikely that a lawsuit would ever have been filed.

Ultimately, providing prompt notice whenever a data breach occurs avoids violating state law notice requirements and discourages the filing of class actions.

--By Kevin M. McGinty, Mintz Levin Cohn Ferris Glovsky and Popeo PC

Kevin McGinty is a member in Mintz Levin's Boston office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2012, Portfolio Media, Inc.