The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 19783

February 28, 2006

U.S. District Court Dismisses Negligence Suit Based on Company Permitting an Employee to Store Unencrypted Data on Laptop

 [19783] February 28, 2006 TO: PRIVACY ISSUES WORKING GROUP No. 1-06 TECHNOLOGY ADVISORY COMMITTEE No. 3-06 RE: U.S. DISTRICT COURT DISMISSES NEGLIGENCE SUIT BASED ON COMPANY PERMITTING AN EMPLOYEE TO STORE UNENCRYPTED DATA ON LAPTOP The U.S. District Court for the District of Minnesota has dismissed a lawsuit alleging that a company acted negligently in permitting an employee to keep nonpublic customer data on a laptop computer that was stolen from the employee's home during a burglary.* While this suit originally involved three claims – breach of contract, breach of fiduciary duty, and negligence – the first two of these claims were voluntarily dismissed. Accordingly, the only claim before the court was negligence. As discussed in more detail below, after analyzing the defendant's duty of care to the defendant – including its duty under the privacy protections of the Gramm-Leach-Bliley (GLB) Act and its own privacy policy – the court held that the defendant did not act negligently and dismissed the plaintiff's claim with prejudice. FACTS OF THE CASE The defendant in this case is a company that originates and services student loans. One employee of the company, who works from his home in Maryland, analyzes loan portfolios, including those containing student loans. As part of his work, this employee requires loan-level details, including customer personal information. In September 2004, the employee's home was burglarized and, among other items, the laptop computer provided to him by the defendant was stolen. Though the matter was reported to the police, the laptop computer was never recovered. The computer contained unencrypted customer personal information, though the defendant was unable to determine with any degree of certainty which customers' information was on the laptop when it was stolen. As a result, the defendant sent a notification letter to all of its approximately 550,000 customers alerting them to the theft. To the defendant's knowledge, none of its customers experienced any type of fraud or identity theft as a result of the theft of the computer. * See Guin v. Brazos Higher Educ. Svc., Civ. No. 05-668 (RHK-JSH) (Feb. 7, 2006). A copy of the case is available at: http://www.nysd.uscourts.gov/courtweb/pdf/D08MNXC/06-00529.PDF. 2 THE COURT'S ANALYSIS The plaintiff alleged the defendant breached its duty of care under both the GLB Act and the defendant's own privacy policy by failing to secure the plaintiff's private personal information. As a result of this alleged negligence, the plaintiff suffered out-of-pocket losses, emotional distress, fear and anxiety, and other damages. In response, the

defendant argued that it did not breach any duty it owed to the plaintiff, the plaintiff did not sustain an injury, and the plaintiff could not establish proximate cause. In its analysis, the court first considered whether the defendant breached its duty of care under the GLB Act by permitting the employee to continue keeping personal information in an unattended, insecure personal residence and allowing the employee to keep unencrypted customers' personal information on his laptop. It concluded that the plaintiff did not present "sufficient evidence from which a fact finder could determine that [the defendant] failed to comply with the GLB Act." In reaching this conclusion, the court noted "the GLB Act does not prohibit someone from working with sensitive data on a laptop computer in a home office. Despite [the plaintiff's] persistent argument that any nonpublic personal information stored on a laptop computer should be encrypted, the GLB Act does not contain any such requirement." The plaintiff also claimed that the defendant failed to comply with the "self-imposed reasonable duty of care" in the defendant's privacy policy, which stated that the defendant would restrict access to nonpublic personal information to authorized persons on a "needs to know" basis. The defendant argued that it handled the plaintiff's personal information with reasonable care, and the court agreed. It noted that the customers' data was transmitted and used according to the defendant's policies; the defendant's employee lived in a relatively safe neighborhood and took necessary precautions to secure his house from intruders; and his inability to foresee and deter the burglary was not a breach of the defendant's duty of reasonable care. The court next addressed the plaintiff's arguments that he was injured by the defendant's conduct and the defendant's conduct was the proximate cause of such injuries. On the first of these arguments, the court found that the plaintiff was unable to present evidence that his data was targeted or accessed by the burglars or that he experienced any identity theft or other fraud involving his personal information. As such, it concluded, "no genuine issue of material fact exists concerning whether [the plaintiff] suffered an injury." In response to the second argument, the court concluded that the theft of the laptop was not reasonably foreseeable to the defendant. While the Minnesota Supreme Court had previously observed that a high crime rate and the commission of similar crimes in a particular area can establish foreseeability of a subsequent criminal attack, those facts were not present in this case. Accordingly, the court held that "[a] reasonable jury could not infer that the burglary caused [the plaintiff] any alleged injury; such a conclusion would be the result of speculation and conjecture, not a reasonable inference." Tamara K. Salmon Senior Associate Counsel

---