Security of Employees' Personal Information Focus of New Ninth Circuit Case

I have been following a case concerning an employer's obligation to protect employee data that has now come to a conclusion with two Ninth Circuit decisions. Krottner et al. v. Starbucks arose from the 2008 theft of a laptop that contained the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees. On November 19, 2008, Starbucks sent a letter to affected employees alerting them to the theft and stating that Starbucks had "no indication that the private information has been misused." Nonetheless, the letter continued:

> As a precaution, we ask that you monitor your financial accounts carefully for suspicious activity and take appropriate steps to protect yourself against potential identity theft. To assist you in protecting this effort [sic], Starbucks has partnered with Equifax to offer, at no cost to you, credit watch services for the next year.

This situation resulted in filed two nearly identical putative class action complaints against Starbucks, alleging negligence and breach of implied contract. On August 14, 2009, the district court granted Starbucks's motion to dismiss, holding that the Plaintiffs had standing under Article III but had failed to allege a cognizable injury under Washington law. The Ninth Circuit issued two separate opinions, one for publication and one not for publication, that affirmed the lower court's ruling. The opinion for publication [http://www.ca9.uscourts.gov/opinions/view_subpage.php?pk_id=0000011050] dealt with the standing issue. In analyzing the issue the Court applied a four-part test for standing: (1) 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. It was undisputed that the second and third parts of the test had been met. In analyzing the first prong, the Court noted that one of the Plaintiff's alleged injuries were "generalized anxiety and stress," which was sufficient to confer standing. The other Plaintiff's allegations concerned their increased risk of future identity theft. After considering the decisions of several other courts, the Ninth Circuit concluded that if a plaintiff faces "a credible threat of harm," and that harm is "both real and immediate, not conjectural or hypothetical," the plaintiff has met the injury-in-fact requirement for standing under Article III. Thus, the Plaintiff's had alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data. The court noted that if the allegations had been more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future— it would have found the threat far less credible.

While that opinion was good news for the Plaintiffs, the unpublished opinion was not. In that opinion [http://www.ca9.uscourts.gov/datastore/memoranda/2010/12/14/09-35823.pdf], the Court held that the Plaintiff did not adequately allege the elements of their state law claims. The Court noted that their conclusion that the Plaintiffs had standing to sue did not necessarily mean that they had adequately pled damages for their substantive claims. Under state law, the negligence claims required actual loss or damage; the threat of future harm is insufficient. Although one Plaintiff alleged that someone *attempted* to open a bank account in his name, he did not allege that he suffered any actual harm. The arguments that alleged anxiety was an actionable injury was waived by the Plaintiffs and not considered. As to the other claim, breach of implied contract, the Court concluded that it to was not adequately pled. The Plaintiffs had pointed to three documents but did not allege that they had read or even saw the documents, or that they understood them to be an offer. Thus, the Ninth Circuit affirmed the lower court's decision to dismiss the case.

As implied by the Ninth Circuit's election to publish one opinion and not the other, the important part of this case is the standing issue. The Ninth Circuit has gone along with the Seventh Circuit in specifically extending standing to potential harm in the case of identity theft. This holding is consistent with decisions from the Second, Fourth, Sixth and Ninth Circuits granting standing for potential injuries in the context of toxic substance, medical monitoring and environmental claims. The takeaway from this case is that the door is wide open for lawsuits against employers who do not adequately protect employee data. In this particular case, the Plaintiffs did not have sufficient facts

(or did not plead them) to make it past a motion to dismiss. In the future, I suspect that Plaintiffs' attorneys will do a better job developing facts and drafting pleadings, making if more difficult to dispose of such cases.

What can you do to avoid claims? First, review security procedures and practices with your technology group. Consider using encryption software and other security measures for employee laptops. Second, review data security procedures with human resources. Is it really necessary for any employee to be carrying significant amounts of employee data on a laptop? If not, leave it in the workplace; if so, put procedures in place to protect the data. Assuming one of these cases makes it past the pleading stage, the unlucky employer being sued will need to demonstrate that reasonable care was exercised to protect employees. Can you meet that standard?

.