ALERT
MARCH 13, 2012

GLOBAL INSURANCE GROUP
News Concerning
Recent Professional Liability Issues

COZEN O'CONNOR
www.cozen.com

WHEN IT COMES TO DATA BREACHES: SHOW ME THE INJURY

Andrea Cortland • 215.665.2751 • *acortland@cozen.com*
Stephanie P. Gantman • 215.665.2116 • *sgantman@cozen.com*

Two recent decisions, one by Oregon's highest court and the other by the 1st Circuit Court of Appeals, reveal a growing trend finding legitimacy in claims asserted by plaintiffs whose personal information has been stolen or compromised *only if* such information is actually used by a third-party to cause harm or perpetuate identity theft. In other words, a data breach *alone* does not constitute injury giving rise to recoverable damages – there must be use of the information stemming from the data breach.

In *Paul v. Providence Health System-Oregon*, the Supreme Court of Oregon addressed whether a health provider was liable for damages when the provider's negligence allowed theft of patients' personal information, but the information was never used or viewed by a third-party. --- P.3d ---, 2012 WL 604183 (Or. Feb. 24, 2012). In *Paul*, the plaintiffs alleged that their health care provider was negligent in allowing the theft of unencrypted computer disks and tapes containing names, social security numbers, and clinical information for approximately 365,000 patients. The plaintiffs sought both economic and non-economic damages for financial injury and emotional distress.

The *Paul* court presumed, without deciding, that a health care provider owed a duty to protect its patients from economic loss and a duty to protect patient information. The court then focused on plaintiffs' failure to allege an actual, present injury that resulted in economic loss. The court found the threat of future harm was insufficient. In explaining its rationale, the court analogized this case to nationwide case law – including 3rd and 7th Circuit opinions – rejecting claims for credit monitoring damage in the absence of actual identity theft or other harm. *See Pisciotta v. Old Nat'l Bancorp,* 499 F.3d 629 (7th Cir. 2007) (rejecting bank customers' negligence claims for credit monitoring data accessed, but not used, by a hacker); *Reilly v. Ceridian Corp*., 664 F.3d 38 (3rd Cir. 2011) (holding increased risk of identity theft did not establish injury for purposes of credit monitoring expenses).

The *Paul* court did not mention on-point precedent from the 9th Circuit, which supports the Oregon Supreme Court's determination. *See Krottner v. Starbucks*, 628 F.3d 1139 (9th Cir. 2010) (finding that when a computer containing employees' personal information was stolen, Washington law does not recognize a cause of action where the sole damage alleged is "risk of future harm"). The *Paul* court then distinguished *Anderson v. Hannaford Bros. Co*., 659 F.3d 151 (1st Cir. 2011), where damages were awarded when stolen personal information was used to perpetuate identity theft. As the *Paul* court suggested, the facts underlying the theft in *Hannaford* – which is reportedly one of the largest data breaches in history – were crucial to *Hannaford's* holding. In that case, there was more than just a threat of harm; the plaintiffs' credit card data was actually misused by those who stole it.

Much like the Oregon Supreme Court, the 1st Circuit Court of Appeals reached a similar conclusion in *Katz v. Pershing, LLC*, No. 11-1983 (1st Cir. Feb. 28, 2012). *Katz* addressed whether the plaintiff, who maintained an account with a company for which the defendant provided brokerage clearing services, had standing to bring various claims against the defendant for the defendant's alleged failure to protect sensitive non-public personal information. Specifically, the plaintiff alleged that the electronic platform used by the defendant

allowed all users to access customers' non-public personal information, such as social security, taxpayer identification and bank account numbers, and therefore, the risk of this information being compromised was high. The court noted, "the plaintiff's concern is that her non-public personal information has been left vulnerable to prying eyes because it is inadequately protected by the defendant's service." The court dismissed the plaintiff's claims in part because the plaintiff did not allege actual injury. In other words, without any reference to an identified breach of the plaintiff's data security, the court found the plaintiff could not demonstrate a sufficient injury giving rise to Article III standing.

Where do these recent decisions and other opinions addressing stolen or compromised personal information leave us? There is a growing trend to find damages for stolen information compensable only when such information is actually used to perpetuate harm by a third-party. Whether this trend will continue, or if courts in other jurisdictions will reach differing conclusions, remains to be seen.

To discuss any questions you may have regarding the issues discussed in this alert, or how they may apply to your particular circumstances, please contact Stephanie P. Gantman at 215.665.2116 or sgantman@cozen.com or Andrea Cortland at 215.665.2751 or acortland@cozen.com. Both Stephanie and Andrea are members of Cozen O'Connor's Professional Liability Coverage Practice Group.