The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 20, No. 2 February 2012

First Circuit Decision Opens The Door For Data Breach Suits

Bruce L. McDonald and Kirk J. Nahra

WILEY REIN LLP

Businesses may wish to take special note of the First Circuit's October 20 decision in *Anderson v. Hannaford Brothers Co*. (2011 U.S. App. Lexis 21239), because it could well open the door for class actions against companies that suffer data breaches. Thus, it may signal an end to the heretofore consistent rulings foreclosing such litigation.

The Breach And Prior Proceedings

As understood by the courts, Hannaford, a national grocery chain, suffered a security breach of its electronic payment-processing system by hackers beginning as early as December 7, 2007. Hannaford was notified by Visa, Inc. on February 27, 2008 that there had been a breach, and, by March 10, Hannaford contained the breach. On March 17, it announced publicly that the system had been breached, leading to the theft of as many as 4.2 million debit and credit card numbers belonging to individuals who had made purchases at more than 270 of its stores. Moreover, Hannaford had received reports of approximately 1,800 cases of fraud resulting from the theft of those numbers.

Numerous responsive actions were taken by cardholders, card issuers and others, and numerous proposed class actions were filed against Hannaford and affiliated companies. Twenty-six of these were consolidated by the Judicial Panel on Multidistrict Litigation in the District of Maine, thus creating a major proceeding.

The plaintiffs alleged a laundry list of

Bruce L. McDonald

Kirk J. Nahra

supposed legal theories for granting relief and sought to recover for numerous types of loss, inconvenience and expenditure. In May 2009, presiding Judge D. Brock Hornby granted Hannaford's motion to dismiss the complaint for failure to state a claim upon which relief can be granted under Maine law, which ruling essentially would have ended the multidistrict action. He ruled that some of the pleaded causes of action were not recognized under Maine law, and those that were recognized must be dismissed because the types of damages claimed by the named plaintiffs were not ones that are recoverable under Maine law.

Thereafter, he certified certain questions to the Maine Supreme Judicial Court. Last year, the Maine court ruled that "time and effort alone, spent in a reasonable effort to avoid or remediate reasonably foreseeable harm" are *not* injuries for which damages may be recovered under Maine negligence or implied contract law. In that context, both the plaintiffs and Hannaford appealed to the U.S. Court of Appeals for the First Circuit.

The First Circuit's Decision

Chief Judge Sandra L. Lynch's opinion, joined in by Circuit Judges Juan R. Torruella and O. Rogeriee Thompson, considered first the theories of recovery that might be applicable under Maine law and ruled that both negligence and implied contract could apply (and rejected "fiduciary duty" and the Unfair Trade Practices Act). The court denied Hannaford's appeal and ruled that a jury could reasonably find an implied contract between Hannaford and its credit or debit card customers that Hannaford "would take reasonable measures to protect the information" on the cards.

Chief Judge Lynch then turned to the key issues of "cognizable injury." The Court of Appeals noted that Maine law allows for recovery of mitigation expenses that are "foreseeable," subject

Please email the authors at bmcdonald@wileyrein.com or knahra@wileyrein.com with questions about this article.

to policy considerations, such as "societal expectations regarding behavior and individual responsibility in allocating risks and costs." It noted that Maine had adopted Restatement (Second) of Torts § 919, which provides in part that one "whose legally protected interests have been endangered by the conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened." The key is whether the expenditures were "reasonably made," which, under Maine law, means whether the decision to mitigate was reasonable "at the time it was made."

Chief Judge Lynch found no Maine decisions bearing on the application of § 919 and then looked to decisions in other jurisdictions. The ones discussed arose from factually far different scenarios, involving construction defects (mitigating damage to locomotive engines, replacing rot-damaged windows, replacing defective stucco on homes and removing a defectively manufactured sewer pipe), not data breaches. In that context, she concluded that "whether plaintiffs' mitigation steps were reasonable" is "a contextual question depending on the facts."

The opinion identified several facts as being relevant to the reasonableness of specific mitigation actions taken by specified named plaintiffs (the proposed class representatives): (1) the breach involved "a large-scale criminal operation," (2) "conducted over three months," (3) with "deliberate taking of credit card and debit card information," (4) "by sophisticated thieves," (5) "intending to use the information to their financial advantage" and (6) who used the data "to run up thousands of improper charges across the globe."

In that context, the court found reasonable two types of mitigation expenditures alleged to have been made by named plaintiffs. One was the cost of replacing cards, alleged by two plaintiffs who had not experienced unauthorized charges. Another was the expenditure by a named plaintiff who had experienced unauthorized charges to purchase "insurance to protect against the consequences of data misuse." It reversed the dismissal insofar as needed to reinstate the named plaintiffs' negligence and implied contract claims for those expenditures.

The Path To More Litigation

That ruling itself is pretty narrow, but it appears to hold the seeds for further expanding such litigation. The court's analysis of what mitigation steps might be reasonable was focused by the particular steps the named plaintiffs here alleged they had taken. The opinion did not, however, rule out approval of recovering the costs of other mitigation steps that might have been taken by other plaintiffs (*e.g.*, the purchase of credit-monitoring services).

Also leading toward more claims is the framework of analysis under which the reasonableness of a mitigator decision depends on the facts and appears to be a subjective determination made by the presiding judge. The court here noted six facts as contributing to the plaintiffs' mitigation decisions being reasonable, but it did not say that all six facts were essential to making those decisions reasonable. Nor did it rule out the possibility that other types of facts could support a reasonableness decision. Would replacing credit cards be reasonable if naive thieves working locally for a short period of time obtained numerous card numbers and then used them to run up thousands of improper charges? Only time will tell, but this decision certainly leaves the possibility open.

Obviously, one compelling fact here was that Hannaford's announcement said there already had been 1,800 reported cases of fraudulent use of the card numbers. However, the court did not say that the actual fraudulent use of the cards was a necessary prerequisite to a reasonable decision to mitigate. So the opportunity is there for a judge to find a mitigation step to have been reasonable in the absence of fraudulent use at the time that step was taken.

These factors, together with the Maine negligence and implied contract legal principles not being unusually favorable to plaintiffs, suggest that decisions allowing putative class actions to seek recovery of costs of mitigation steps following disclosure of a data breach may become much more common. At least, we should expect plaintiffs' counsel to cite the *Hannaford* decision in support of such initiatives.

Bruce L. McDonald's *practice focuses on business litigation. He also has particular experience in copyright enforcement, emerging privacy issues and in federal and state regulation of food, drugs, medical devices and environmental hazards, including product liability issues, as well as the Commerce Clause and First Amendment implications of product marketing. He has been named by* Corporate Counsel *magazine for excellence in business litigation and repeatedly recognized in the* Best Lawyers in America *directory for distinction in commercial litigation.*

Kirk J. Nahra *specializes in health care, privacy, information security, compliance programs and insurance fraud issues for the health care and property/casualty insurance industries and others facing legal obligations on these issues. He served as the co-chair of Confidentiality, Privacy and Security Workgroup, a panel of government and private sector privacy and security experts advising the American Health Information Community (AHIC). Rated by* Chambers USA *in the nation's top tier of privacy attorneys, sources praise Mr. Nahra as "a fantastic lawyer who keeps abreast of new developments in the field" who "avoids legal jargon and goes the extra mile for his clients" (2011) and commend him for both his "tremendous knowledge of current data privacy and security law" and his "practical knowledge of what other health care organizations are doing and how they are interpreting the law" (2010). Mr. Nahra has been named an expert practitioner by the* Guide to the Leading U.S. Healthcare Lawyers, *a leading health care lawyer by* The Best Lawyers in America *directory and one of the leading privacy "hired guns" by* Computerworld.