PERSPECTIVES

RESPONSES TO REGULATORY ENFORCEMENT AND CLASS ACTIONS ARISING FROM DATA BREACHES: TOO LITTLE, TOO LATE?

BY **NANCY KELLY AND COLIN N. HOLMES**
> GOVERNO LAW FIRM LLC

Seemingly every day there is news of another cyber attack or breach of private information. In the past two months alone we learned one identity theft ring accessed credit card or email data from several large companies, including Cupid Media, PR Newswire, Adobe and LexisNexis, affecting millions of individuals. More importantly, cybercrime shows no sign of abating, as hackers adapt to new technologies and become increasingly savvy at accessing private information. This rise in cybercrime, and the attendant media coverage, has resulted in a corresponding increase in the number of regulatory enforcement actions filed by the Federal Trade Commission (FTC), as well as a wave of consumer class actions. Companies face a substantial risk of financial and reputational harm from data breaches and related litigation. Businesses are nevertheless fighting back against such suits, by contesting the FTC's authority to bring enforcement

actions and challenging class actions based on several legal theories.

In the past few years, the FTC has initiated nearly 50 enforcement actions for data security violations. The vast majority of these actions have resulted in settlements that include large fines and require businesses to meet specific cyber security criteria and submit to audits. The FTC brings these regulatory actions for data breaches under the general authority of Section 5 of the FTC Act, which prohibits businesses from engaging in "unfair or deceptive acts or practices in or affecting commerce". The FTC interprets this language as authorising it to ensure that companies are adequately protecting private consumer information. Recently, however, two companies have challenged the FTC's authority to bring such actions.

In the first such case, *Federal Trade Commission v. Wyndham Worldwide Corporation*, No. CV 12-1365-PHX-PGR, filed in 2012, the FTC brought suit against a hotel chain, alleging that it did not sufficiently protect private customer information after hackers gained access to credit and debit card data. Wyndham filed a motion to dismiss the case, arguing that Section 5 does not authorise the agency to regulate data security. During oral argument on 7 November 2013, District Judge Salas noted that if Congress had not intended to grant the FTC such authority, it would have acted years ago to pass specific legislation granting the FTC or another organisation the power to bring such actions. This exchange suggests that there is judicial support for the FTC, however the Court's decision is pending. A second case, *In the matter of LabMD, Inc.*, No. 9357, filed in 2013, made similar claims contesting the FTC's authority. In that action the FTC brought suit against a laboratory for failing to protect personal data on a file sharing network found in the hands of identity thieves. A hearing is scheduled in April before an administrative court. These two cases exemplify a greater willingness by businesses to challenge regulatory actions rather than acquiesce to the FTC's demands; however it is likely that these courts will uphold the FTC's right to bring such actions.

> "In the past few years, the FTC has initiated nearly 50 enforcement actions for data security violations."

In addition to an increase in the number of regulatory actions, there has been a significant upsurge in the number of civil data privacy class actions being filed. In many jurisdictions companies

have successfully challenged these actions based on class members' lack of standing. 'Standing' is the basic legal principle that for an individual or class to bring suit there must be: (i) actual or imminent harm; (ii) a causal connection between the injury and the conduct; and (iii) a likelihood that a ruling will redress the injury.

Class actions are often filed shortly after a data breach is disclosed to the public, once plaintiffs' firms have enlisted individuals whose data was lost to bring suit. In many of these cases there is no evidence that the information was ever used by hackers or that the class suffered any actual harm. Instead, the class argues that the loss of private data constitutes a *risk* of imminent harm sufficient to meet the injury requirement and confer standing. Recent decisions before the First and Third Circuits, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) and *Katz v. Pershing, LLC*, 672 F.3d 64, 78 (1st Cir. 2012), rejected this argument and dismissed such actions, holding that plaintiffs lacked standing because the risk of future harm is not sufficient to meet this standard. However, the Ninth and Seventh Circuits, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) and *Pisciotta v. Old Nat. Bancorp.*, 499 F.3d 629 (7th Cir. 2007), have ruled that plaintiffs had standing based on an increased risk of identity theft as a result of the breach. Until the issue is resolved by the Supreme Court, there is a circuit court split, with the risk that courts in other jurisdictions may find standing in data breach cases.

Defendants also have pursued other avenues to get cases dismissed, usually based on an absence of actual damages. In *Pisciotta*, plaintiffs did not allege that they suffered any direct financial loss or identity theft as a result of the data breach. The Court, in dismissing the case, rejected an argument that the potential cost to plaintiffs of future credit monitoring constituted present damages. Likewise in *Krottner*, the Court ruled that plaintiffs had standing, but dismissed the case for failure to adequately plead the claims for negligence and breach of contract. The Court held, in part, that plaintiffs failed to show any damages related to their negligence claim. Therefore even in cases where standing was found, defendants' additional arguments resulted in dismissals of class actions.

Companies also challenge data privacy class actions by contesting 'certification'. The Federal Rules require a class to meet several requirements for it to be certified and the case to proceed. One such requirement is predominance – questions of law or fact for the class as a whole must predominate over questions affecting individual members. In a recent Maine District Court case, *In re Hannaford Bros. Privacy Litig.*, 2:08-MD-1954-DBH (D.Me., Mar. 20, 2013), a class action was brought on behalf of customers of a grocery store chain whose credit card data was stolen. The Court found that there were common questions of fact regarding the incident, but that individual questions of damages predominated. The class claimed that they had incurred card charges due to the theft; however the Court determined that an individual assessment of damages would be necessary, since some cardholders incurred charges for reasons unrelated to the theft. Thus the court ruled that individual questions predominated and dismissed the action.

Another case, however, in the Northern District of Illinois, *Harris v. comScore, Inc.*, No. 11-C-5807 (N.D.Ill., Apr. 2, 2013), granted class certification in a data breach class action. *Harris* was brought by customers of comScore who alleged that the company unlawfully collected data on their internet activity and sold it to third parties. The suit sought statutory damages under several privacy statutes that mandated minimum fines for violations, making damages easier to calculate than in *In re Hannaford Bros.* The Court determined that because individual damages were small, it was unlikely that individuals would file suit outside of a class action. Even with the necessity of individual damages hearings, the Court concluded that a class action was the most efficient and fair means of resolving the case. This ruling evidences that class certification has been interpreted differently by the courts and challenging certification is not a surefire defence.

Regulatory enforcement and litigation can result in significant legal fees, civil damages and settlements, regulatory fines and the spectre of costly mandatory audits by regulatory agencies. Publicity stemming from data breaches can also impair a business's reputation. The best course of action is to reduce these risks in the first place. There are several steps companies can take to minimise the likelihood of data breach, limit potential liability and manage cyber risk. Companies should routinely update their data privacy policies to comply with relevant regulations and protect confidential information. Such policies should include regular attorney-directed risk assessments that evaluate existing data protection measures to ensure compliance with the legal and regulatory framework and identify any problems before they happen. Businesses should also establish methods to assess data breaches if they occur, to quickly evaluate the harm and potential liability. It is also important to create incident-response teams to respond to data privacy breaches by identifying the cause, complying with

applicable regulations, and minimising negative effects on potential regulatory investigations and collateral civil litigation. Companies should also consider their coverage portfolios and consider purchasing cyber liability insurance, which can mitigate the costs of data breaches. Expending resources on data security preventative and responsive measures in the first instance is less costly than facing costly investigations, fines and litigation after a data breach has occurred.

The financial and reputational costs of data breaches can be devastating for a business. Even though companies are challenging regulatory enforcement and class actions based on a number of different legal theories, conflicting decisions abound and new cases will continue to be filed based on novel legal theories as plaintiffs firms adapt to rulings. Businesses should be proactive by taking steps to reduce the chance of a breach and to maintain a response plan for such breaches. It is generally accepted that the prevention of data breaches is an impossible goal. Instead, the best practice is to focus on reducing the likelihood of harm. RC

Nancy Kelly
Partner
Governo Law Firm LLC
T: +1 (617) 532 9214
E: nkelly@governo.com

Colin N. Holmes
Associate
Governo Law Firm LLC
T: +1 (617) 737 9930
E: cholmes@governo.com