Compliance & Ethics Professional®

April 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Mark Lanterman

Chief Technology Officer
Computer Forensic Services
Minnetonka, MN

See page **14**

by Keith M. Gerver and Peter T. Carey

Marketing and Data Security Practices: The *FTC v. LifeLock* settlement

» The LifeLock settlement reinforces the FTC's emergence as a leading cybersecurity regulator.
» The FTC is committed to enforcing its orders, including those involving data security.
» The consequences of violating an FTC order can be severe.
» Compliance with industry data security standards, although important, may not insulate companies from liability.
» Companies should assess carefully their data security practices and their representations about such practices.

On December 17, 2015, the Federal Trade Commission (FTC or the Commission) announced that LifeLock, Inc. (LifeLock) had agreed to settle contempt charges that the company violated the terms of a 2010 federal court order. That order requires LifeLock to establish and maintain a comprehensive information security program and prohibits the company from misrepresenting its identity-theft protection services. The settlement, which is the largest monetary award obtained by the FTC in an order enforcement action, "demonstrates the Commission's commitment to enforcing the orders it has in place against companies, including orders requiring reasonable security for consumer data."[1]


Gerver


Carey

The FTC action

In 2010, the FTC initiated an enforcement action against LifeLock in the United States District Court for the District of Arizona, alleging that the company used false claims to promote its identity-theft protection services and made false claims about its own data security. On March 9, 2010, LifeLock and the FTC announced they had reached a settlement. As part of the settlement, LifeLock consented to a Stipulated Final Judgment and Order for Permanent Injunction (the 2010 Order), pursuant to which it: (1) agreed to pay $11 million to the FTC and $1 million to 35 state attorneys general; (2) is barred from making deceptive claims or misrepresentations about its services; and (3) must establish a comprehensive data security program, obtain biennial third-party assessments of that program, and abide by certain compliance monitoring and recordkeeping requirements.

In August 2013, LifeLock's former Chief Information Security Officer, Michael Peters, filed whistleblower complaints with the FTC, SEC, and U.S. Department of Labor relating to LifeLock's allegedly insufficient compliance with the 2010 Order. Accordingly, on January 17, 2014, LifeLock met with the FTC regarding

regarding Peters' allegations. On February 4, 2015, LifeLock provided the FTC with a $20 million settlement offer; however, the FTC rejected this offer. LifeLock's CEO, Todd Davis, later told investors that the FTC action could result in LifeLock facing "hundreds of millions of dollars" in liability.

On July 21, 2015, the FTC filed under seal a motion for contempt against LifeLock in the United States District Court for the District of Arizona. The motion alleged that LifeLock violated the 2010 Order, and the FTC's sealing notice, which is public, explained the FTC's allegations that LifeLock: (1) failed to establish a comprehensive information security program; (2) made false claims about the security of its customers' data; (3) failed to meet the 2010 Order's record-keeping requirements; and (4) made false claims about how quickly it provided identity theft-related alerts to its customers.

On October 28, 2015, LifeLock announced that it had reached a comprehensive settlement agreement with the Commission and plaintiffs in a related class action lawsuit.

On October 28, 2015, LifeLock announced that it had reached a comprehensive settlement agreement with the Commission and plaintiffs in a related class action lawsuit. Although LifeLock told investors it was setting aside $116 million to cover the two proposed settlements, the terms of the settlements, which still required approval from the Commission and relevant courts, were not released at the time. Those terms became public on December 17, 2015, when the FTC announced that LifeLock had agreed to pay $100 million to settle the contempt charges. Under the terms of the settlement, in which LifeLock neither admitted nor denied it had violated the 2010 Order, $68 million of the $100 million is to be used to pay redress to the plaintiffs as part of a settlement of a related class action lawsuit, discussed in more detail below. The remaining $32 million will fund consumer redress ordered by any state attorneys general, with any money not being used for that purpose reverting to the FTC for use in further consumer redress. In addition, LifeLock agreed to reporting, monitoring, and record-keeping requirements similar to those in the 2010 Order.

The Commission vote approving the settlement was 3-1, with Commissioner Maureen Ohlhausen voting no. Commissioner Ohlhausen dissented on the grounds that there was not clear and convincing evidence that LifeLock failed to establish and maintain the required information security program. She pointed specifically to third-party certifications that LifeLock complied with the Payment Card Industry Data Security Standard (PCI DSS) and other data security standards. Chairwoman Edith Ramirez, Commissioner Julie Brill, and Commissioner Terrell McSweeny said that Commissioner Ohlhausen's focus on third-party certifications was misguided, referring to the Commission's "longstanding view that PCI DSS certification is insufficient in and of itself to establish the existence of reasonable security protections… . [T]he existence of a PCI DSS certification is an important consideration in, but by no means the end of,

[the Commission's] analysis of reasonable security."[2] In this case, the majority found that the evidence "fully justifie[d]" bringing contempt charges against LifeLock.

Related litigation and enforcement actions

In addition to the FTC's contempt charges, LifeLock has faced several other lawsuits and enforcement actions related to its marketing practices and alleged violation of the 2010 Order. These include a nationwide class action suit alleging deceptive marketing and sales practices, two purported securities fraud class actions, a whistleblower complaint brought by LifeLock's former Chief Information Security Officer, and state attorneys general investigations.

On January 19, 2015, plaintiffs filed a class action complaint alleging that LifeLock's marketing and sales practices violated the Arizona Consumer Fraud Act.

LifeLock's settlement of the FTC's contempt charges is part of a comprehensive settlement agreement that also resolves the nationwide class action (i.e., *Ebarle v. LifeLock, Inc.)*, which alleged deceptive marketing and sales practices in connection with LifeLock's identity-theft protection services. On January 19, 2015, plaintiffs filed a class action complaint alleging that LifeLock's marketing and sales practices violated the Arizona Consumer Fraud Act. The plaintiffs alleged, for example, that LifeLock could not place fraud alerts on customers' credit files as described in its advertising. As described above, $68 million of the $100 million LifeLock agreed to pay to resolve the FTC's contempt charges is authorized to fund an escrow account in *Ebarle* to pay redress to affected consumers.

On July 21, 2015, United States District Court Judge Susan R. Bolton dismissed with prejudice a purported securities class action filed against LifeLock in March 2014 in United States District Court for the District of Arizona. The consolidated amended complaint in that action (i.e., *In re LifeLock, Inc. Securities Litigation*) alleged that LifeLock and its senior executives violated Sections 10(b) and 20(a) of the Securities Exchange Act by making materially false or misleading statements, or failing to disclose material facts regarding certain of LifeLock's business, operational, and compliance policies, including with regard to certain of LifeLock's services, its data security program, and LifeLock's compliance with the 2010 Order. In dismissing the complaint, Judge Bolton found that the only statement the plaintiffs could identify relating to LifeLock's compliance with the 2010 Order ("[O]ur business is subject to the FTC [Order] . . . , as well as the companion orders with 35 states' attorneys general that we entered into in March 2010. We incur significant costs to operate our business and monitor our compliance with these laws, regulations, and consent decrees."[3]) was not misleading because it only described the costs LifeLock incurred in complying with the 2010 Order and did not "'affirmatively create an impression' that LifeLock was actually in compliance with the [2010] Order."[4]

But on July 22, 2015—the day after *In re LifeLock, Inc. Securities Litigation* was dismissed and the FTC contempt action was filed—a second class-action complaint was filed against LifeLock in the United States District Court for the District of Arizona. The complaint in

this case, *Avila v. LifeLock, Inc.*, alleges that LifeLock and its CEO and CFO violated Sections 10(b) and 20(a) of the Securities Exchange Act by making materially false or misleading statements, or failing to disclose material facts about LifeLock's business, operations, and prospects, including about LifeLock's information security program and its compliance with the 2010 Order. A lead plaintiff was appointed and an amended class action complaint making substantially similar allegations to those in the July 22, 2015 complaint was filed on December 10, 2015. A hearing on LifeLock's motion to dismiss the amended class action complaint is scheduled for May 2, 2016. LifeLock's settlement of the FTC's contempt charges may improve the plaintiffs' case in *Avila*.

On March 20, 2014, Michael Peters, LifeLock's former Chief Information Security Officer, filed a complaint against LifeLock in the United States District Court for the District of Arizona alleging that LifeLock violated the whistleblower protection provisions of the Sarbanes-Oxley Act and the Dodd-Frank Act by terminating his employment as a result of his disclosures to management about LifeLock's information security practices. Peters claimed to have performed an initial risk assessment that determined, *inter alia*, that "LifeLock's security vigilance (e.g. vulnerability testing, auditing, monitoring, awareness education, event logging, incident management, etc.) was at 0% of the minimum to protect LifeLock's customers and their sensitive information."[5] LifeLock and Peters reached an undisclosed settlement in October 2015, and the case was dismissed on November 25, 2015.

In addition to the terms of the 2010 Order, LifeLock is bound by the companion orders it entered into with 35 states' attorneys general imposing injunctive provisions similar to those in the 2010 Order.

The LifeLock settlement stands out, however, as the Commission's most aggressive enforcement to date of an order requiring reasonable data security practices

Analysis

The FTC's expanding role in policing businesses' data security practices and the Commission's record of bringing contempt cases against parties who do not comply with the terms of their settlements with the FTC are two trends that have been publicized for several years. The LifeLock settlement stands out, however, as the Commission's most aggressive enforcement to date of an order requiring reasonable data security practices. As FTC Chairwoman Edith Ramirez said, "This settlement demonstrates the Commission's commitment to enforcing the orders it has in place against companies, including orders requiring reasonable security for consumer data."[6] There are several notable takeaways for businesses and practitioners tracking the FTC's evolving regulation of data security practices.

First, if a business violates an FTC order, the financial impact can be severe. The FTC made headlines in 2012 when it announced a then-record $22.5 million settlement with Google Inc. resolving claims that the company violated a 2011 settlement

agreement by misrepresenting to users of the Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users. The LifeLock settlement significantly raises the bar. In addition to the record $100 million settlement, the terms of the agreement require that every LifeLock employee sign a statement acknowledging receipt of a copy of the 2010 Order and the December 17, 2015 settlement agreement. As the related litigation discussed above also demonstrates, an FTC enforcement action can result in significant fallout in other forums.

Second, the Commission has put businesses on notice that compliance with the PCI DSS "is insufficient in and of itself to establish the existence of reasonable security protections."[7] The PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. The Commission endorsed the PCI DSS in its recent settlement with Wyndham Hotels and Resorts,[8] and Commissioner Ohlhausen noted in her statement dissenting from the Commission's approval of the LifeLock settlement that LifeLock obtained third-party certification that it complied with the PCI DSS and other data security standards. But in *LifeLock*, the Commission made clear that "PCI DSS certification is an important consideration in, but by no means the end of, [the FTC's] analysis of reasonable security."[9] As to what additional steps the FTC might expect businesses to take beyond PCI DSS compliance, the Commission in *LifeLock* pointed to additional terms in the Wyndham settlement, including "the implementation of risk assessments, certification of untrusted networks, and certification of the assessor's independence and freedom from conflicts of interest."[10]

Conclusion

This most recent settlement between the FTC and LifeLock in relation to LifeLock's violation of the 2010 Order provides another important opportunity for businesses to evaluate their data security practices to ensure the protection of consumer data and the accuracy of their representations regarding those practices. As the Commission made clear, compliance with certain industry standards may not be sufficient to show that a business has established reasonable data security protections. The settlement also reinforces the FTC's emergence as a leading cybersecurity regulator, as it demonstrates that the Commission will keep a close watch over the actions taken and statements made by businesses with which it has settled data security-related actions. LifeLock's experiences further highlight the need for businesses to plan for the related actions that will likely follow in the wake of an FTC enforcement action. Companies should be prepared not only for the filing of class action lawsuits wherever they may find affected customers, but also for possible whistleblower actions related to the treatment of employees who internally report concerns about data security practices. ✳

1. Federal Trade Commission press release: "LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order" December 17, 2015. Available at http://bit.ly/lifelock-to-pay
2. Statement of the Federal Trade Commission at 1-2, *FTC v. LifeLock, Inc.*, December 17, 2015. Available at http://bit.ly/ftc-lifelock
3. LifeLock, Inc., Annual Report (Form 10-K) 12. February 26, 2013.
4. *Bien v. LifeLock, Inc.*, No. CV-14-00416-PHX-SRB, at 4 (D. Ariz. Jul. 21, 2015).
5. Complaint at 5, *Peters v. LifeLock, Inc.*, 2:14-cv-00576-ROS (D. Ariz. filed Mar. 20, 2014).
6. Ibid., *supra* note 1.
7. Ibid., *supra* note 2, at 2.
8. Federal Trade Commission, press release: "Wyndham Settles FTC Charge It Unfairly Placed Consumers' Payment Card Information at Risk" December 9, 2015. Availabe at http://bit.ly/Wyndham-Settles
9. *Id.*
10. *Id.*

Keith M. Gerver *(keith.gerver@cwt.com) and* ***Peter T. Carey*** *(peter.carey@cwt.com) are Associates in Cadwalader's White Collar Defense and Investigations Group, based in Washington DC.*