Chicago Daily Law Bulletin®

Volume 162, No. 48 Serving Chicago's legal community for 161 years

FTC plays hard ball, fines LifeLock for violating customer privacy order

The Federal Trade Commission recently demonstrated that it doesn't fool around when a business violates an order requiring it to improve security measures with customer personal information.

Ironically, the company in question is LifeLock, a provider of identity theft protection services.

LifeLock must pay $100 million — the largest monetary penalty the agency has ever levied in an order-enforcement action — to settle contempt charges for violating a 2010 court order. The 2010 order was intended to settle a lawsuit filed in an Arizona federal court by the FTC and the attorneys general of 35 states including Illinois, accusing LifeLock of deceptive advertising practices and failing to secure customers' personal data.

"While LifeLock promised consumers complete protection against all types of identity theft, in truth, the protection it actually provided left enough holes that you could drive a truck through it," then-FTC Chairman Jon Leibowitz said in a 2010 statement.

The settlement also required LifeLock to pay a fine of $12 million — $11 million to the FTC and $1 million to the state attorneys general — and to take tougher measures to protect customers' personal information.

In addition, the order prohibited LifeLock from making deceptive advertising claims.

LifeLock apparently didn't follow through, and the federal government investigated.

The $100 million penalty is no mere slap on the wrist for LifeLock; the company announced last month that its total 2015 revenue was between $586 million to $587 million. And it clearly demonstrates the FTC's readiness to crack down — hard — on businesses that flout the agency's authority.

The previous record for an FTC order-enforcement penalty was $22.5 million (against Google in 2012 for breaking its promise not to install tracking cookies on Safari users' computers). This settlement with LifeLock is in a whole different sphere, given its substantially higher price tag.

The harshness reflects not only the company's failure to adhere to the previous settlement, but also that the company failure to fulfill its responsibilities as a provider of identity theft protection services.

"The fact that consumers paid LifeLock for help in protecting their sensitive personal information makes the charges in this case particularly troubling," FTC Chairwoman Edith Ramirez noted in a statement on Dec. 17, 2015.

The FTC asserts that LifeLock violated the 2010 order by failing to establish and maintain a comprehensive information security program and compounded the violation by falsely advertising that it protected consumers' sensitive data with the same high-level safeguards used by financial institutions.

The contempt suit also alleges that LifeLock did not follow the record-keeping requirements of the 2010 order and falsely advertised that it would send alerts "as soon as" it received any indication that a consumer may be a victim of identity theft.

According to the FTC's complaint, LifeLock has stated in its advertisements: "By now you've heard about individuals whose identities have been stolen by identity thieves. ... LifeLock protects against this ever happening to you. Guaranteed." LifeLock has also stated: "Do you ever worry about identity theft? If so, it's time you got to know LifeLock. We work to stop identity theft before it happens."

According to the FTC, the fraud alerts Lifelock placed on customers' credit files protected them against only certain forms of identity theft. Fraud alerts warn creditors opening new accounts "to take reasonable measures to verify that the individual applying for credit actually is who he or she claims to be, but in some instances, identity thieves can thwart even reasonable precautions," the FTC explained in the complaint.

While these fraud alerts are most effective in protecting new accounts, new account fraud constitute less than 20 percent of identity theft incidents, according to the agency.

Fraud alerts provided no protection against the misuse of existing accounts, which is the most common type of identity theft. Contrary to LifeLock's claims, complete protection, even for the types of identity theft for which fraud alerts are most effective, cannot be guaranteed, according to the agency.

Further, the FTC maintained LifeLock did not protect customers from medical identity theft or employment identity theft in which hackers steal personal information to get medical care or apply for jobs.

LifeLock advertised that it would prevent unauthorized changes to customers' address information, that it constantly monitored activity on customer credit reports, and that it would ensure a customer always received a telephone call from a potential creditor before a new account was opened.

According to the complaint, the FTC's investigation determined those claims were all false.

Perhaps most egregious, however, was that the FTC found LifeLock's own internal data security practices to be inadequate. LifeLock, which routinely collected customers' personal information, including their Social Security numbers and credit card numbers, promised in its advertising: "All stored personal data is electronically encrypted." It also claimed: "Only authorized employees of LifeLock will have access to the data that you provide to us, and that access is granted only on a 'need to know' basis."

According to the FTC, these claims weren't true, either. The agency determined that LifeLock's data was not encrypted and sensitive consumer information was not shared only on a need-to-know basis, making LifeLock's own data system was vulnerable.

To settle the contempt charges, LifeLock must deposit $100 million with the Arizona federal court, of which $68 million will be used to reimburse fees paid to LifeLock by customers injured as a result of the company's violations, including the settlement of a consumer class action in Arizona related to the same advertising and data security claims.

The remaining $32 million will go toward settlements between LifeLock and the state attorneys general. In addition, the record-keeping provisions instituted in 2010 have been extended to 13 years from the date of the original order.

In a statement, LifeLock said, "As a part of the settlement, LifeLock neither confirms nor denies the allegations of the parties."

The company also pointed out: "The allegations raised by the FTC are related to advertisements that we no longer run and policies that are no longer in place. The settlement does not require us to change any of our current products or practices. Furthermore, there is no evidence that LifeLock has ever had any of its customers' data stolen, and the FTC did not allege otherwise."

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law as well as intellectual property law, focusing on trademark clearance and counseling.