LOEB & LOEB LLP

Privacy

JUNE 2015

Staying Out of the FTC's Data Security Cross-Hairs

by Ieuan Jolly, Partner

As the Federal Trade Commission acknowledges in a recent blog post, no company wants to discover that its data security practices are under federal investigation. Yet any company that collects, uses or maintains consumer data could be the subject of a formal or informal investigation. And while not all FTC investigations lead to enforcement actions, investigations can be costly in terms of resources dedicated to responding to FTC requests for information and leave companies at risk of further FTC action that can cause reputational and monetary damages.

In its blog post "If the FTC comes to call," the Commission outlined the steps involved in data security investigations and emphasized the Commission's focus: whether a company's data security practices are reasonable - under the company's particular circumstances - and whether companies follow through on what they promise in their privacy and data security policies.

The FTC initiates investigations either on its own or based on a wide variety of information from a number of sources - including news reports, consumer complaints or complaints from other companies, and requests from Congress or other agencies. Any company that handles consumer data may be the subject of an investigation. Most investigations begin informally - with the FTC reviewing publicly available information or sometimes reaching out to the company directly. And in some instances the investigation ends there, with no further action by the Commission.

If the FTC determines that it needs to take an informal review to the next level, it often notifies the company of the commencement of the formal investigation through a letter requesting more information. The Commission looks for: documents and information related to the company's policies and practices, including audits or risk assessments that the company or its service providers have performed, the company's information security plan, privacy policies and any other promises the company has made to consumers about its security, as well as employee handbooks and training materials. The FTC may also request interviews with employees with knowledge about the company's data security practices, and may also look to people outside the company, such as experts, consumers and employees of other companies, including vendors.

The focus of the information gathering is on "what a company says about its data security practices -

as well as what it actually does," and whether the company's practices are "reasonable in light of the sensitivity and volume of consumer information the company holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."

As the FTC's recent enforcement action and settlement with Nomi Technologies (read our alert on the Nomi Technologies settlement here) illustrates, the Commission also looks closely at whether companies "keep their promises" by adhering to their own privacy and data security policies and procedures, and the representations they make to consumers. If a company is in an industry subject to additional regulation, such as the Gramm-Leach-Bliley Act or the Fair Credit Reporting Act, the FTC may also look at company policies to evaluate compliance with those regulations.

If the investigation is prompted by a data security breach, the focus of the investigation will be on the likely or actual harm the breach may have caused to consumers: "[W]e're focused on the security of consumer information entrusted to the company - not its IP portfolio, trade secrets, or the loss of other company information that doesn't concern consumers." Other important factors include whether the company was forthcoming in reporting the breach, took actions to assist affected consumers and cooperated with law enforcement agencies.

If, after review of all of the information, the FTC staff believes that the company has violated the law, it will make a recommendation to the Commission to proceed with an administrative action or complaint in federal court, and may attempt to negotiate a settlement with the company. While investigations - whether formal or informal - generally are not made public and do not necessarily indicate that a company has violated the law, they can be costly in terms of the diversion of resources to answering the Commission's requests for documents and other materials, and employee testimony. Not all investigations lead to enforcement actions, but some do, and enforcement actions and settlements may be the subject of FTC press releases and other publicly available information, subjecting the company to public scrutiny and reputational damage, as well as further costs and potential damages.

So, when the FTC comes knocking, will you be ready? Now is the time to review, revise and update your information security program and audit your data-handling practices to ensure you are complying with your policies and legal obligations. A regulatory inquiry does not necessarily mean prosecution if companies institute policies, procedures and protocols that are appropriate to their size and business - and then take steps to follow them.

For more information about risk mitigation strategies, data security compliance and information governance programs, please contact Ieuan Jolly at ijolly@loeb.com.

Advanced Media and Technology Practice

KENNETH A. ADLER	KADLER@LOEB.COM	212.407.4284
ELIZABETH J. ALLEN	EALLEN@LOEB.COM	312.464.3102
AMIR AZARAN	AAZARAN@LOEB.COM	312.464.3330
IVY KAGAN BIERMAN	IBIERMAN@LOEB.COM	310.282.2327
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
MARC CHAMLIN	MCHAMLIN@LOEB.COM	212.407.4855
MEG CHARENDOFF	MCHARENDOFF@LOEB.COM	212.407.4069
ALESON CLARKE	ACLARKE@LOEB.COM	310.282.2240
PATRICK N. DOWNES	PDOWNES@LOEB.COM	310.282.2352
CRAIG A. EMANUEL	CEMANUEL@LOEB.COM	310.282.2262
KENNETH R. FLORIN	KFLORIN@LOEB.COM	212.407.4966
DANIEL D. FROHLING	DFROHLING@LOEB.COM	312.464.3122
NOREEN P. GOSSELIN	NGOSSELIN@LOEB.COM	312.464.3179
DAVID W. GRACE	DGRACE@LOEB.COM	310.282.2108
NATHAN J. HOLE	NHOLE@LOEB.COM	312.464.3110
MELANIE J. HOWARD	MHOWARD@LOEB.COM	310.282.2143
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
CAROL M. KAPLAN	CKAPLAN@LOEB.COM	212.407.4142
ELIZABETH H. KIM	EKIM@LOEB.COM	212.407.4928
JANICE D. KUBOW	JKUBOW@LOEB.COM	212.407.4191
JULIE E. LAND	JLAND@LOEB.COM	312.464.3161
JESSICA B. LEE	JBLEE@LOEB.COM	212.407.4073
SCOTT S. LIEBMAN	SLIEBMAN@LOEB.COM	212.407.4838
DAVID G. MALLEN	DMALLEN@LOEB.COM	212.407.4286
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA COYLE MCGINN	NMCGINN@LOEB.COM	312.464.3130
ANNE KENNEDY MCGUIRE	AMCGUIRE@LOEB.COM	212.407.4143
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
BRIAN NIXON	BNIXON@LOEB.COM	202.618.5013
ELISABETH O'NEILL	LONEILL@LOEB.COM	312.464.3149
SUE K. PAIK	SPAIK@LOEB.COM	312.464.3119
ANGELA PROVENCIO	APROVENCIO@LOEB.COM	312.464.3123
KELI M. ROGERS-LOPEZ	KROGERS-LOPEZ@LOEB.COM	310.282.2306
SETH A. ROSE	SROSE@LOEB.COM	312.464.3177
ROBERT MICHAEL SANCHEZ	RSANCHEZ@LOEB.COM	212.407.4173
ALISON SCHWARTZ	ASCHWARTZ@LOEB.COM	312.464.3169
BARRY I. SLOTNICK	BSLOTNICK@LOEB.COM	212.407.4162
BRIAN R. SOCOLOW	BSOCOLOW@LOEB.COM	212.407.4872
AKIBA STERN	ASTERN@LOEB.COM	212.407.4235
JAMES D. TAYLOR	JTAYLOR@LOEB.COM	212.407.4895
JILL WESTMORELAND	JWESTMORELAND@LOEB.COM	212.407.4019
DEBRA A. WHITE	DWHITE@LOEB.COM	212.407.4216
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960