LOEB & LOEB LLP

Privacy

JULY 2015

FTC's New Consumer Data Security Guidance Offers Businesses Practical Tips

by Ieuan Jolly, Partner and Nerissa McGinn, Partner

The Federal Trade Commission has issued new guidance on data security for companies that collect, store and use consumer information, gleaned from the more than 50 enforcement actions brought by the agency over the past decade. The guidance, "Start with Security: A Guide for Business," distills 10 "lessons learned" from data security lapses, illustrating each lesson with a specific settlement.

1. Start with security. Securing confidential consumer information must be part of the decision-making process of every part of the organization, including personnel, sales, accounting and information technology. Businesses also should make informed choices about what information to collect, how long to keep that information and when to use it. The FTC suggests that "less" is preferable in all of these areas, advising against collecting "unnecessary" personal information, storing that information any longer than needed and using personal information in situations where it isn't warranted.

2. Control access to data sensibly. Employees should have access to consumer information on a "need to know" basis according to their job functions, and controls can take the form of anything from password-protected user accounts that limit network access to locked file cabinets.

3. Require secure passwords and authentication. Strong authentication procedures help ensure that only authorized individuals are able to access sensitive data. According to the FTC, however, companies too often fail to follow basic precautions like insisting that employees and customers use complex and unique passwords and ensuring passwords are securely stored. The agency also recommends companies maintain security of their authentication mechanisms by regularly testing for common vulnerabilities.

4. Store sensitive personal information securely and protect it during transmission. In addition to storing personal information, many companies transmit it to others. The FTC recommends using strong cryptography to secure confidential material during storage and transmission. The agency also advises that businesses must secure sensitive information for the entire duration of its use — from transmissions from the customer's web browser to the business's website server during collection, and during storage and retransmission or use.

This publication may constitute "Attorney Advertising" under the New York Rules of Professional Conduct and under the law of other jurisdictions.

5. Segment networks and monitor who is trying to get in and out. The FTC recommends tools including firewalls to segment business networks, and intrusion detection and prevention tools to monitor networks for malicious activity.

6. Secure remote access to networks. According to the FTC, a mobile workforce creates increased security risks, and businesses that give employees, clients or service providers remote access to their networks must secure those access points, including ensuring appropriate endpoint security by insisting that clients take basic security measures such as installing firewalls and updated antivirus software before accessing their networks and putting sensible access limits in place, such as limiting third-party access to networks by restricting connections to specified IP addresses or granting temporary, limited access.

7. Apply sound security practices when developing new products. A new app or software may require customers to store or send sensitive information. FTC cases involving product development, design, testing and rollout indicate that some businesses didn't think through how their new product would handle this data securely. The FTC recommends training engineers in secure coding practices to avoid vulnerabilities, following platform guidelines for security, verifying that privacy and security features work as advertised to customers, and adequately testing products for well-known vulnerabilities.

8. Make sure service providers implement reasonable security measures. The guidance recommends that companies investigate and monitor the data security practices of any third-party providers, communicating clear expectations about security (including making those expectations part of the service contract), selecting providers that are able to implement the appropriate security measures and verifying compliance.

9. Put procedures in place to keep security current and address vulnerabilities that may arise. The FTC advises that securing software and networks is an ongoing process and that detecting and addressing vulnerabilities in a product or third-party software requires constant vigilance. Once a problem has been detected, businesses must move quickly to fix it.

10. Secure paper, physical media and devices. The security of physical media, including paper files, hard drives, laptops, flash drives and disks, is as critical as network security, and the FTC recommends that businesses securely store sensitive files and not leave them out in the open or keep them in unsecured areas. Organizations must also protect devices that collect and process personal information, like PIN entry devices, and keep safety standards in place when sensitive data is en route by tracking mailed packages, limiting instances when employees need to travel with sensitive data in their possession, and training employees to secure sensitive data when traveling.

For more information, please contact Ieuan Jolly at ijolly@loeb.com or Nerissa McGinn at nmcginn@loeb.com.

This alert is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

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	310.282.22240
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
MEREDITH SILLER	MSILLER@LOEB.COM	310.282.2294
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