CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

THURSDAY, SEPTEMBER 24, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 187

FTC gives words of warning to the wise

The Federal Trade Commission has issued new guidance on data security to help businesses that collect, store and use consumer information to stay out of hot water with the agency.

Gleaned from the more than 50 enforcement actions the FTC brought in the past decade, the guidance — "Start with Security: A Guide for Business" — offers lessons for building an effective data security strategy and reducing the risk of data breach. It also illustrates the fundamental mistakes that led to the enforcement actions.

1. Start with security.

Many businesses collect, process and store confidential customer information. The FTC suggests that securing this information properly should be part of the decision-making process of every part of the business — not just information technology, but also human resources, sales and accounting, among other departments. To minimize risk, businesses also should make truly informed choices about consumer information, including what to collect, how long to keep that information and when to use it.

According to the FTC, one of the lessons learned through its enforcement actions is that less is better when it comes to consumer data. What's more, the agency advises against collecting unnecessary personal information, storing it longer than needed and using it in unwarranted situations.

2. Control access to data sensibly.

Not everyone in an organization needs access to sensitive data. The FTC recommends that employees have access on a need-to-know basis. Access control can take the form of anything from having user accounts that limit network access to locking file cabinets.

To illustrate the access lesson, the FTC points to its settlement with Goal Financial, in which the agency alleged that Goal Financial failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. Proper controls ensuring that only authorized employees with a business need had access to consumers' personal information would have prevented the breach.

Moreover, the guidance suggests that restricting administrative access to network systems based on job requirements reduces the risk that a compromise of an employee's credentials could result in a serious breach.

3. Require secure passwords and authentication.

Strong authentication procedures help ensure that only authorized individuals are able to access sensitive data. Too often, companies fail to follow the most basic precautions, leaving them vulnerable to hackers.

For example, the agency filed charges against Reed Elsevier for letting customers store user credentials in a vulnerable format in cookies on their computers. The FTC says organizations must insist that employees and customers use complex and unique passwords and ensure passwords are securely stored. Businesses must also protect against "brute force attacks" by hackers using automated programs to figure out passwords. The agency also recommends companies maintain security of its authentication mechanisms by regularly testing for common vulnerabilities.

4. Store sensitive personal information securely and protect it during transmission.

Many companies have to both store sensitive data and send it to third parties. The FTC advises using strong cryptography to secure confidential material during storage and transmission. Keeping sensitive information secure for the duration of its use is critical.

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. She can be reached at nmcginn@loeb.com.

The FTC pointed to Superior Mortgage Corp., which used encryption to secure the transmission of data between the customer's Web browser and its Web server, but failed to protect the information once it reached the server. The company's service provider decrypted it and e-mailed it in readable text to the company's headquarters.

The guidance recommends that companies use only industry-tested and accepted encryption methods and ensure those methods are properly configured.

5. Segment your network and monitor traffic.

The guidance recommends using tools such as firewalls to segment your network and intrusion detection and prevention programs to monitor your network for malicious activity.

For example, when shoe retailer DSW failed to sufficiently segment its network, hackers were able to access one in-store network to connect with other in-store and corporate networks and access personal information.

When Cardsystem Solutions failed to monitor its network activity, according to the FTC, hackers were able to install programs that collected sensitive data and sent it outside the Cardsystem network every four days.

6. Secure remote access to your network.

A mobile workforce poses increased security challenges, and businesses that give employees, clients or service providers remote access to their networks must secure those access points. FTC enforcement cases suggest a few factors to consider when developing remote access policies. Businesses must ensure appropriate endpoint security by insisting that clients take basic security measures such as firewalls and updated anti-virus software before accessing their networks.

Settlement One and Lifelock are two examples of companies that failed to take this basic precaution, according to the FTC. Sensible access limits must be in place as well. Some organizations neglect to limit third-party access to their networks, which can be done 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 do not properly address security when introducing new products. The guidance recommends training engineers in secure coding practices to avoid vulnerabilities, following platform guidelines for security, verifying that privacy and security features work as advertised and adequately assessing and testing products for known vulnerabilities.

8. Make sure service providers implement security measures.

Third-party service providers are a particular vulnerability. Businesses need to be clear about expectations and select providers that are able to implement the appropriate security measures. The guidance recommends making security standards part of the service contract and to not rely on verbal assurances from a provider about security.

The FTC pointed out GMR Transcription, which hired service providers to transcribe sensitive audio files but failed to require the providers to take reasonable security measures.

9. Set procedures to keep your security current and address potential vulnerabilities.

The guidance explains that securing software and networks is an ongoing process and detecting and addressing vulnerabilities requires constant vigilance. Failing to regularly update anti-virus software increases the risk that hackers could exploit known vulnerabilities or breach a business' defenses. And once a problem has been detected, businesses must move quickly to fix it.

10. Secure paper, physical media and devices.

Network security is critical but so is the security of physical media: paper files, hard drives, laptops, flash drives and disks. Organizations also must protect devices that collect and process personal information, like PIN entry devices. Organizations should keep safety standards in place when sensitive data is en route by tracking packages, limiting instances when employees need to travel with sensitive data in their possession and training employees to secure sensitive data when traveling.

Other FTC initiatives

To reinforce its commitment to data security, the FTC is launching several initiatives, including a new website featuring the agency's data security information for businesses (ftc.gov/datasecurity) with information about enforcement cases, reports, education and advocacy filings and holding free one-day security conferences for businesses.