Privacy & Security @ MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy & Security Alert

JUNE 11, 2012

Federal Trade Commission Brings Two Enforcement Actions Related to Peer-to-Peer Networks

BY CYNTHIA J. LAROSE AND AMY MALONE

The Federal Trade Commission (FTC) has brought two separate enforcement actions aimed at companies that improperly shared information over peer-to-peer (P2P) networks, putting, according to the FTC's press release, the information of thousands of consumers at risk. In both cases, the respondents failed to secure their networks, which led to customers' personal information being exposed. The FTC found in each case that these failures of security constituted unfair trade practices. Again, the FTC has provided business with clear roadmaps to what is, and what is not, acceptable information security.

EPN

EPN, Inc. is a debt collector based in Utah specializing in collecting hospital bills. According to the FTC's complaint, EPN failed to implement many important business practices and failed to use reasonable methods to prevent, detect, and investigate unauthorized access to its networks. As a result, EPN's chief operating officer was able to install P2P software, which caused a breach affecting approximately 3,800 hospital patients. The information accessed included each patient's name, address, date of birth, Social Security number, employer name, employer address, health insurance number, and a diagnosis code. The FTC found these practices in violation of Section 5(a) of the FTC Act as an unfair act or practice.

The FTC consent order bars EPN from misrepresenting how it maintains and protects client privacy, confidentiality, and security. EPN is also required to establish and maintain an information security program and conduct testing and risk assessments to pin-point areas of weakness and concern. In addition to its own assessments, EPN must also obtain independent data security audits every other year for 20 years.

Franklin Toyota

Franklin Toyota is a car dealership in Georgia that sells and leases cars and provides financing for its customers. According to the FTC's complaint, Franklin Toyota failed to secure a P2P network, which caused a breach affecting 95,000 consumers. The information exposed included consumer names, Social Security number, addresses, dates of birth, and drivers' license numbers. Franklin Toyota was found to be in violation of section 5(a) of the FTC Act (unfair or deceptive practice) for not taking reasonable measures to protect consumer information and failing to implement policies and procedures to prevent this unauthorized disclosure in direct violation of its privacy policy.

In addition to the FTC Act, Franklin Toyota was found to be in violation of the Gramm-Leach-Bliley Act (GLB) Safeguards and Privacy rules as it is a "financial institution" as defined under GLB. Franklin Toyota failed to have a written information security plan and it did not provide an opt-out for their sharing of nonpublic consumer information with nonaffiliated third parties. According to the FTC's announcement, this is the agency's first GLB action against an auto dealer.

Franklin Toyota's consent order requires it to develop and maintain a security plan and an opt-out mechanism for consumers as well obtaining a third-party audit of its security measures every other year for 20 years.

What Does this Mean for You?

P2P technology is a low cost way for companies to build an internal network; however, there are many risks. If you decide to build your network using P2P technology, make sure your company has written information security policies in place and that all employees are trained on those policies. Also, P2P applications are downloaded by employees without permission or knowledge of systems administrators. These applications (as in the case of EPN) can expose all information on a network. Restrictions and blocks should be implemented to prevent employees from adding P2P applications to any corporate system that could expose sensitive information to the Internet. The FTC has posted a helpful informational discussion of risks of P2P networks and information sharing on its "Business Center Blog."

When sensitive personal information is to be shared and stored, serious consideration should be given to the acceptability of the risk of that information being put on a P2P network and whether that level of risk can be managed. It is important to remember that once the information has been shared by the P2P application it often cannot be removed, even after the information has been deleted from the original source. *Any* computer that is connected to that network – anywhere – has access to the shared files. Read Peer-to-Peer File Sharing: A Guide for Business, published by the FTC. Proper information security procedures and training of employees on those procedures are the best ways to ensure the information you have on your corporate network won't be improperly accessed.

These cases also drilled home the fact that the FTC continues to examine privacy policies and to work to ensure that companies are protecting and sharing information as outlined in those policies. Risk assessment is always a good time to review your information security and information sharing practices and make sure they both are in harmony with what you say in your privacy policy.

* * *

View Mintz Levin's Privacy & Security attorneys.

Read and subscribe to ***Privacy & Security Matters*** blog.