Shook, Hardy & Bacon L.L.P.

JUNE 14, 2012

DATA SECURITY ALERT

CAN A COMPANY BE LIABLE FOR ITS EMPLOYEE INSTALLING FILE-SHARING SOFTWARE?

The Federal Trade Commission (FTC) has charged and settled with two businesses that exposed their consumers' personal information via peer-to-peer (P2P) file-sharing software installed on their networks. The lessons learned about a company's obligation to control and monitor software installed on its network are invaluable.

P2P software is commonly used to play games, make online telephone calls, and share software and documents. The software is sometimes used to share and download (often illegally) movies and music. If not configured correctly, files not intended for sharing may be accessible to anyone on the P2P network. So, for example, an employee may install P2P software on her desktop, download/share a hit song via the software, and inadvertently expose customer information also residing on the employee's desktop. Once shared, the information can be difficult to remove from the P2P network.

The FTC Chairman, Jon Leibowitz, has previously warned that "[c]ompanies should take a hard look at their systems to ensure that there are no unauthorized P2P file-sharing programs and that authorized programs are properly configured and secure. Just as important, companies that distribute P2P programs . . . should ensure that their software design does not contribute to inadvertent file sharing."

In the first lawsuit filed by the FTC, an auto dealer allegedly compromised its consumers' personal information by allowing P2P software to be installed on its network, which led to sensitive financial information being uploaded to the P2P network. The FTC claimed that the auto dealer failed to implement "reasonable security measures" such as:

- assessing risks to the consumer information it collected and stored
- adopting policies to prevent or limit unauthorized disclosure of information
- preventing, detecting, and investigating unauthorized access to personal information on its networks
- adequately training employees
- responding to unauthorized access to personal information

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

SHB guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage risks associated with maintaining and using electronic information.

For more information on SHB's data security and data privacy services, please contact:

Al Saikali
(305) 960-6923
asaikali@shb.com

- because the dealer is also a financial institution, it is governed by the Gramm-Leach-Bliley Safeguards Rule, and accordingly failed to provide annual privacy notices and provide a mechanism by which consumers could opt out of information sharing with third parties.

In the FTC's second lawsuit, a debt collection company was charged with failing to implement reasonable security measures after the company's Chief Operating Officer installed a P2P application on her desktop computer that allowed the private information of 3,800 individuals to leak into P2P network. The FTC's complaint details actions the debt collection company allegedly failed to take:

- failure to adopt an information security plan that was appropriate for its network and the personal information processed and stored on them
- failure to implement an incident response plan
- failure to assess risks to the consumer information collected and stored online
- failure to adequately train employees about security to prevent unauthorized disclosure of personal information
- failure to assess and enforce compliance with its existing security policies and procedures, such as scanning networks to identify unauthorized P2P file sharing applications and other unauthorized applications operating on the networks or blocking installation of such programs
- failure to prevent, detect, and investigate unauthorized access to personal information on its networks, such as by logging network activity and inspecting outgoing transmissions to the Internet to identify unauthorized disclosures of personal information.

The FTC entered into settlement agreements in both lawsuits and, in both instances the agreements require the defendants to, among other things, establish and maintain a comprehensive information security program and undergo data security audits by independent auditors every other year for 20 years.

What are the lessons for Corporate America? First, these lawsuits are warnings that the FTC will hold companies responsible for software that employees install on company-issued devices if the software poses threats to consumer personal information. Second, P2P or other file-sharing software can pose a threat to personal information, so companies should control and monitor the use of such file-sharing software by their employees. Third, as the FTC settlements demonstrate, companies must be proactive and undergo audits of their information security network, adopt information security policies and procedures, train their employees, and remain vigilant against threats to personal information stored on company networks **before** a data breach occurs.

For further information about the FTC action, visit:
http://www.ftc.gov/opa/2012/06/epn-franklin.shtm

Al blogs about developments in data security law at:
http://www.datasecuritylawjournal.com

OFFICE LOCATIONS

Geneva, Switzerland
+41-22-787-2000
Houston, Texas
+1-713-227-8008
Irvine, California
+1-949-475-1500
Kansas City, Missouri
+1-816-474-6550
London, England
+44-207-332-4500
Miami, Florida
+1-305-358-5171
San Francisco, California
+1-415-544-1900
Tampa, Florida
+1-813-202-7100
Washington, D.C.
+1-202-783-8400