

**FTC PROBE DISCOVERS WIDESPREAD DATA BREACH INVOLVING
PEER TO PEER SHARING AND PROVIDES GUIDANCE TO BUSINESSES
ON PROTECTING SENSITIVE INFORMATION**

Overview

A wide-ranging Federal Trade Commission (“FTC”) probe has uncovered data breaches at nearly 100 public and private organizations of sensitive information¹ of customers and/or employees resulting from the use of peer-to-peer (“P2P”) file sharing networks, where the information may be vulnerable for use in identity theft or fraud. As a result, the FTC has published detailed guidance on how an organization can address the security risks posed by the widespread availability of P2P technology.²

P2P Technology

Computers with P2P software installed are able to share various digital files, including documents, music, video and games, with other users over a network and to facilitate online telephone conversations. Examples of common P2P file sharing programs include BearShare, LimeWire, KaZaa, eMule, Vuze, uTorrent and BitTorrent.

Security Risks of P2P Technology and the FTC’s Findings

Users of P2P file sharing software can inadvertently share files containing customer or employee sensitive information that they may not intend to share with others over a network outside of their organization. Unintended file sharing may occur by accidentally choosing to share drives or folders that contain sensitive information, or by saving a private file to a shared drive or folder by mistake, thereby making that private file available to others. In addition, viruses and other malware can cause files designated as private to be inadvertently shared over a network. Additionally, P2P software flaws or vulnerabilities may open up a computer to attacks from other computers on the network.

FTC Response to Findings of Probe

As a result of the FTC probe, the FTC has sent breach notification letters to a number of organizations and in some other cases has opened nonpublic investigations. Such organizations comprised both large and small public and private organizations, including schools and local governments.

¹ Sensitive information includes Social Security numbers, credit card and account information, and medical and other personal data.

² <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm>

Summary of FTC Recommendations and Guidance

The first step in formulating a program to address P2P file sharing is for an organization to decide whether it will ban or allow the use of file sharing programs on its computers.

If an organization decides to ban the use of file sharing programs, it should

- Prevent P2P file sharing programs and any unapproved programs from being installed on its network by using administrative security controls to block access to sites where such programs can be downloaded.
- Detect P2P file sharing programs already installed and block traffic associated with them by using scanning tools, network monitoring and access restricting tools and data loss prevention tools, and by reviewing records of activity logs.
- Protect sensitive information by restricting the locations of such information, as well as by using less obvious file names, and, by employing encryption where possible.

If an organization decides to allow the use of file sharing programs, it should

- Control the installation of approved P2P file sharing programs by providing the approved program directly to authorized users from an internal server as opposed to getting it from a public download site.
- Control the use of approved P2P file sharing programs by updating them with the latest security patches, as well as by blocking files with sensitive information from being shared, and by using tools to detect unapproved P2P file sharing programs.
- Protect sensitive information.

Additionally, the FTC recommends that the following general measures be taken to protect sensitive information if an organization allows remote access, including by employees and service providers, to its networks:

- Company computers should be provided to employees rather than allowing them to use their own personal computers.
- Remote access to an organization's network should be allowed only through secure connections such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL) software.
- The locations to which files containing sensitive information can be saved or copied should be restricted, and such files should not be remotely downloaded unless they will be securely deleted when not being used.

- Due diligence should be exercised when allowing third parties to remotely access an organization's network to ensure that appropriate security policies and procedures for addressing P2P file sharing risks are employed.

An organization's employees who have access to files containing sensitive information should also be trained on the security risks associated with P2P file sharing programs. An organization's security measures should be evaluated and monitored to determine if they need to be modified to account for P2P file sharing programs or for changes in circumstances, as well as for hardware and software updates.

* * * * *

If you have any questions regarding this memorandum, please contact Martin R. Miller (212-728-8690, mmiller@willkie.com) or Marc J. Lederer (212-728-8624, mlederer@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

April 8, 2010

Copyright © 2010 by Willkie Farr & Gallagher LLP.

All Rights Reserved. This memorandum may not be reproduced or disseminated in any form without the express permission of Willkie Farr & Gallagher LLP. This memorandum is provided for news and information purposes only and does not constitute legal advice or an invitation to an attorney-client relationship. While every effort has been made to ensure the accuracy of the information contained herein, Willkie Farr & Gallagher LLP does not guarantee such accuracy and cannot be held liable for any errors in or any reliance upon this information. Under New York's Code of Professional Responsibility, this material may constitute attorney advertising. Prior results do not guarantee a similar outcome.