Fox Rothschild LLP
ATTORNEYS AT LAW

Fox Rothschild Podcast

Featuring Litigation Partner John Gotaskie in Pittsburgh

We are talking today about the topic of computer data breaches with John Gotaskie on Fox Rothschild Podcast. John is a partner and litigator with Fox Rothschild in Pittsburgh. He represents clients in diverse legal matters, including complex commercial litigation, creditor's rights and franchising issues as well as social media matters. John, good morning.

John Gotaskie: Good morning. Thank you.

***Question**: John, data breaches seem to be in the headlines practically every day. Customers and the public have really taken notice, and, perhaps more importantly, it seems as though Washington has taken notice.*

John Gotaskie: Yes, that's right. Recently, the FTC initiated an enforcement action alleging data breaches that involved the use of peer-to-peer, or P2P, networks. The action, which resulted in a consent decree, demonstrates that the FTC is watching and unafraid to act. The lesson is deceptively simple: all institutions need to carefully consider their data security practices to ensure legal compliance.

***Question**: John, what do companies really need to know or understand?*

John Gotaskie: Well, let me answer that question by describing a little bit more what happened in the recent FTC case I just mentioned.

***Question:** Sure. What did happen?*

John Gotaskie: According to the FTC complaint, an auto dealer in Georgia, Franklin Toyota, operated a franchised auto dealership. It sells and leases both new and used automobiles and also offers repair services and parts. Importantly, because Franklin Toyota offers financial products such as loans and leases to its customers, it qualifies as a financial institution under the terms of the Gramm-Leach-Bliley Act.

***Question**: John, how did the dealership run afoul of the law?*

John Gotaskie: Well, like many businesses that offer financial products, Franklin Toyota provided customers with statements regarding privacy and data security practices. The dealership's policy was to restrict access to non-public personal information only to those employees who need to know that information—for example to provide products and services to a customer. Franklin Toyota also promised customers that it maintained physical, electronic and

procedural safe guards that comply with federal regulations. Now despite these promises, the dealership did not provide customers with annual privacy notices or a clear and conspicuous opt-out notice explaining their right to prevent the sharing of non-public information.

Question: *John, what types of information did Franklin Toyota collect?*

John Gotaskie: In the course of its normal business, Franklin Toyota routinely collects personal information such as its customers' names, Social Security numbers, addresses, telephone numbers, dates of birth and drivers' license numbers. It stored this information on the company's computer network.

Question*: So why was this a problem?*

John Gotaskie: Because the FTC alleged that Franklin Toyota's security practices were in violation of several laws and rules. These include the FTC Act dealing with unfair or deceptive acts or practices and the Safeguards Rule implementing the Gramm-Leach-Bliley Act requiring financial institutions to protect the security, confidentiality and integrity of customer information. It also involves a Privacy Rule implementing another portion of the Gramm-Leach-Bliley Act requiring financial institutions to provide customers with an initial and then annual notice of its privacy and security policies and practices.

Question*: John, is it fair to say that the dealership was not really protecting a customer's private information at all?*

John Gotaskie: I don't think that's completely accurate. While the FTC asserted a range of claims regarding data security failures, its principal concern regarded P2P networks, which allow file sharing between computer networks. According to the FTC's allegations, Franklin Toyota allowed personal financial information to be made available over such networks.

Now you might know P2P networks as a type of computer program that allows you to commonly exchange music or video files on the web, but they can also be used to exchange all types of computer files. Even more, files shared to a P2P network, even inadvertently, are available to anyone with a computer connected to that network over the internet. Files shared via P2P networks then generally cannot be removed from the network and may live on in that network long after they were deleted from the source computer.

Question*: So John, that placed a lot of customers' personal information at risk?*

John Gotaskie: Indeed. The FTC has been concerned about the sharing of personal data over P2P networks for several years. In fact, in a 2010 report, the FTC stated that a far-reaching investigation showed that entire batches of sensitive, personal information, including health-

related information, financial records and drivers' license and Social Security numbers, had been shared via P2P networks.

The FTC alleged that the failure of Franklin Toyota to employ "reasonable measures" over the installation of the P2P software resulted in the personal information for some 95,000 customers being made available on the internet. Such information could easily have been misused to commit identity theft and fraud.

***Question**: John, how was this remedied?*

John Gotaskie: In brief, Franklin Toyota entered into a proposed consent agreement promising to adhere to both the FTC Act and the Safeguards and Privacy Rules of Gramm-Leach-Bliley. It agreed to design and implement an information security system that protects the sensitive personal information it collects from customers. Franklin Toyota must further designate an employee to coordinate and be accountable for the system.

Also, Franklin Toyota agreed to contract with a qualified expert to conduct periodic written audits of its security systems.

But these are just a few of the expensive and burdensome agreements that the dealership made with the FTC. For those who might want to take a deeper look at the detail, they can review my recent article published in the *Banking & Financial Services Policy Report*.

***Question**: So, John, what would you say are the lessons to be learned?*

John Gotaskie: The number one lesson is prevention and vigilance. Every company, especially those defined as financial institutions by the law, need to develop, implement and monitor how they protect sensitive personal information of consumers. They need to investigate and implement policies and procedures which are commercially reasonable given the size, the scope and the nature of their businesses and the specific threats that business faces.

Regular self-audits of security systems are also necessary to ensure that systems and procedures are keeping up with industry standards and continue to be appropriate for the advancing threats and risks that business faces. It cannot be a program that you "set and forget." Instead, it will need to evolve over time.

***Question**: John, is there anything more that companies need to know?*

John Gotaskie: Yes. Systems are only as good as the people – the employees – who run them. Those employees must be trained on security systems and practices and really understand their importance. Courts have used this measure to decide who should bear responsibility and liability

in recent cases. In one particular case, despite the existence of several layers of electronic security systems and robust security policies, a United States Court of Appeals found that decisions made by bank personnel in violation of best security practices were the reason why a bank failed to catch more than $500,000 in fraudulent bank transfers.

Let's face it. Training is costly, but it's necessary, and courts are likely to conclude that robust education combined with industry standard security practices are the hallmarks of commercially reasonable security practices. In turn, such practices are likely to provide a bulwark against civil liability and a defense, if not a complete solution to, FTC action.

***Narrator**: Well, thank you John. Listeners, to confidentially discuss whether your company may be at risk of security breaches, please contact John at 412-394-5528 or at jgotaskie – that's J-G-O-T-A-S-K-I-E – at foxrothschild.com.*

Fox Rothschild LLP is a full service law firm built to serve business leaders. Over the past 100 years we have grown to more than 500 lawyers in more than 17 offices coast to coast. Our clients come to us because we understand their issues, their priorities and the way they think. We help clients manage risk, and make better decisions by offering practical advice. Visit us on the web at www.foxrothschild.com.

# # # #