MINTZ

Vendor Management Fail: FTC Settles with Mortgage Analytics Company following Vendor Security Issues

January 11, 2021 | Blog | By **Christopher J. Buontempo**, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

An oft-used business management concept is to "hire people smarter than you." The concept also applies to hiring vendors – hire vendors that are *better* than you (especially when it comes to information security). Texas-based Ascension Data & Analytics LLC (Ascension), a technology and data analytics company used by the mortgage industry, did not utilize that concept in its vendor hiring process, and as a result, recently entered into a proposed **settlement agreement** with the Federal Trade Commission (FTC) following charges that it violated the Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule by failing to ensure that its third-party vendor adequately protected mortgage holder personal information.

The FTC Safeguards Rule requires financial institutions under FTC jurisdiction* to protect the security, confidentiality, and integrity of customer information by developing, implementing, and maintaining a comprehensive written information security program that contains administrative, technical, and physical safeguards appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. According to the FTC **complaint** against Ascension, when Ascension hired OpticsML as its third-party vendor, Ascension failed to assess OpticsML's security measures (also in violation of Ascension's own policies). Additionally, the FTC alleged that Ascension's contract with OpticsML failed to adequately require OpticsML to implement appropriate security measures. Finally, the complaint alleged that Ascension failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assess the sufficiency of any safeguards in place to control those risks in connection with its vendor engagement.

The FTC alleged that as a result of Ascension's failures, sensitive personal information of tens of thousands of consumers was exposed to anyone on the internet for a year. During the year that the sensitive personal information was unsecured, approximately 52 unauthorized IP addresses accessed servers and storage locations that contained the sensitive information (most of which were associated with computers outside the United States, including addresses from Russia and China).

The proposed settlement requires Ascension to: 1) implement and maintain a comprehensive data security program with extensive vendor-management requirements; 2) undergo biennial independent assessments of the effectiveness of its data security program, which the FTC has authority to approve; 3) provide annual certifications by an Ascension senior executive that Ascension is complying with the terms of the settlement; and 4) report any future data breaches to the FTC within 10 days of notifying other federal or state government agencies.

In a **press release** announcing the settlement, Andrew Smith, Director of the FTC's Bureau of Consumer Protection was quoted, "Oversight of vendors is a critical part of any comprehensive data security program, particularly where those vendors can put sensitive consumer data at risk. If you're a financial company, vendor oversight is not just a good idea, it's the law."

The settlement provides a valuable vendor management lesson to all business – not just those subject to GLBA. Effective vendor risk management is an absolutely critical component in any business' security program. A business' security program is only as strong as its weakest link, so when engaging vendors, businesses should 'hire better' - and manage appropriately - to ensure that their vendors are not that weak link.

*Other financial regulatory agencies enforce the Safeguards Rule against entities under their regulation, e.g., the Securities and Exchange Commission, the Office of the

Comptroller of the Currency, and the FDIC, and the National Credit Union Administration.

Authors

Christopher J. Buontempo, Associate

Christopher J. Buontempo is a Mintz corporate attorney and a Certified Information Privacy Professional (CIPP). He has significant experience handling issues relating to technology, data privacy and security, brand protection, contract negotiation, licensing, and product development.

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.