VORYS

Publications

FTC Announces Changes to its Standards for Safeguarding Consumer Information

Related Professionals

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 10.29.2021

In a 3-2 decision, the Federal Trade Commission (FTC) announced on Wednesday important updates to its Standards for Safeguarding Customer Information. The updates outline specific practices that the FTC believes will better protect consumer data from ever-increasing cyberattacks and other threats. Notable changes include:

- A requirement that institutions' risk assessments specifically address their criteria for the evaluation of identified security threats, their criteria for the assessment of institutions' information systems and protection of consumer data, how they plan on mitigating or accepting identified risks, and how the their information security programs will address these risks.
- A requirement that institutions' risk assessments be in writing.
- A requirement that financial institutions implement particular safeguards, including access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, testing, and incident response.
- A requirement that institutions select a "Qualified Individual" to manage their information security programs and provide their governing bodies annual reports on their data security practices.
- Expansion of the definition of "financial institution" to include "finders," companies that use sensitive consumer financial information to bring together buyers and sellers of a product or service.

The FTC amended its Standards for Safeguarding Customer Information pursuant to its authority under the 1999 Gramm-Leach-Bailey Act, which mandates that the FTC and other federal agencies establish standards for administrative, technical, and physical safeguards for certain information. Acknowledging that its new Standards may pose unique challenges for smaller entities, the FTC exempted financial institutions that collect information on fewer than 5,000 consumers from its new requirements of a written risk

assessment, incident response plan, and annual reporting to governing bodies.

In a dissenting opinion, Commissioners Noah Joshua Phillips and Christine S. Wilson wrote that the new Standards are "intrusive corporate governance obligations" that will force financial institutions to "divert[] finite resources towards a check-the-box compliance exercise and away from risk management tailored to address individual [institutions'] unique financial needs." Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter, responding in a joint statement, maintained that the amendments are "sorely needed" and asserted that "[t]here is no support for the dissent's notion that the amendments eliminate financial institutions' flexibility in a way that will hurt smaller businesses."

For further information about complying with the FTC's new Standards, or about the law surrounding consumer data protection generally, please contact John L. Landolfi, Christopher L. Ingram, Maxwell H. King, or your Vorys attorney.