CARLTON FIELDS

New York DFS Tightens Cybersecurity Gaps

September 20, 2017

Equifax takes no deposits and makes no loans, but New York now says that it, as well as all other consumer reporting agencies, must protect consumer data to the same degree as banks and other financial institutions. On September 18, the New York Department of Financial Services (DFS) took significant steps in response to the cybersecurity attack at Equifax that compromised the personally identifiable information (PII) of millions of Americans. Among the categories of information compromised were names, Social Security numbers, birthdates, addresses, and, in some cases, drivers' license numbers, as well as the credit card numbers of approximately 209,000 people. Also, in direct response to the Equifax breach, the DFS issued guidance instructing financial institutions to review their information technology, identity theft, and fraud prevention programs. First, the Department, following a directive from Governor Andrew M. Cuomo, proposed new regulations, 23 NYCRR Part 201, requiring all consumer credit reporting agencies (CRAs) reporting on any consumers located in New York to register with the DFS, to comply with certain prohibited practices, and to further comply with the cybersecurity regulation that took effect last month. Previously, CRAs were not "covered entities" under DFS regulations; however, this will change under the proposed regulations, which designate CRAs as "covered entities" subject to the Department's oversight, including its cybersecurity regulation, which took effect last month. Currently, at least 47 consumer reporting agencies are potentially covered by this rule. These entities report consumer information about finances, utility payments, consumer loans, and criminal history. The regulation, entitled "Cybersecurity Requirements for Financial Services Companies" (23 NYCRR Part 500), requires insurance companies and other financial institutions to establish and maintain a cybersecurity program designed to protect consumers and ensure the integrity of New York's financial services industry. The regulation also requires various safeguards including written policies and procedures, a chief information security officer, enhanced cybersecurity controls, and the reporting of cybersecurity events directly impacting a covered entity or those that have a reasonable likelihood of materially harming the normal operations of a covered entity. Second, the DFS issued guidance instructing financial institutions to review their information technology, identity theft, and fraud prevention programs. Noting the unprecedented nature of the attack, the guidance stresses the

critical role that financial institutions will play in the vigilant protection of consumers and financial markets going forward. Specifically, the guidance urges financial institutions to consider taking various security measures, including:

1. the installation of information technology and information security patches,
2. appropriate identity theft and fraud prevention programs for customer due diligence/know your customer (KYC) purposes and before an account is opened or credit or financing is approved,
3. confirmation of the validity of information contained in Equifax credit reports,
4. implementation of a coding system for flagging and monitoring consumer accounts known or suspected to be compromised, and
5. a thorough review for potential risk associated with the continued provision of data to Equifax.

The guidance also recommends the adoption of protective measures such as multi-factor authentication and risk-based authentication techniques, as encouraged by the Department's cybersecurity regulation. This data breach incident, and New York's regulatory response to it, is a harbinger of things to come. The Securities and Exchange Commission (SEC) as well as the Financial Industry Regulatory Authority (FINRA) have previously performed "sweeps" to assess cybersecurity measures, where firms under SEC and FINRA authority received targeted examination letters requiring them to respond to questions related, generally, to their cyber preparedness. State and federal regulators are likely to step up their efforts in this space, as well. Consider whether your firm is ready.

Related Practices

Cybersecurity and Privacy
Financial Services Regulatory
Life, Annuity, and Retirement Litigation
Technology

Related Industries

Technology

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this

publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.