Improving Data Security at Consumer Reporting Agencies

March 26, 2019
|
Download PDF

STATEMENT FOR THE RECORD
FROM CONFERENCE OF STATE BANK SUPERVISORS
TO SUBCOMMITTEE ON ECONOMIC AND CONSUMER POLICY
OF HOUSE COMMITTEE ON OVERSIGHT AND REFORM HEARING
ON "IMPROVING DATA SECURITY AT CONSUMER REPORTING AGENCIES"

The Conference of State Bank Supervisors (CSBS) is the nationwide organization of banking and financial regulators from all 50 states, American Samoa, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. The mission of CSBS is to support the leadership role of state banking supervisors in advancing the state banking system; ensuring safety and soundness; promoting economic growth and consumer protection; and fostering innovative state regulation of the financial services industry.

State regulators charter and supervise 79 percent of all banks in the United States. In addition, state regulators license and supervise a variety of non-bank financial services providers, including fintech, mortgage lending, money transmission, and consumer finance companies. CSBS, on behalf of state regulators, also operates the Nationwide Multistate Licensing System (NMLS) to license and register those engaged in mortgage, money transmission, and other non- bank financial services industries.

CSBS appreciates the opportunity to submit this statement for the record regarding efforts by state regulators related to credit bureaus, and the recent report from the Government Accountability Office titled "Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies." Recently, a number of states conducted a special multi-state examination of Equifax, demonstrating the responsiveness of state regulators and their ability to work together to protect confidential personal information and to improve cybersecurity at consumer reporting agencies.

Consent Order with Equifax

The states have an ongoing interest in the oversight of consumer reporting agencies. In some states, this authority includes direct authority over consumer reporting agencies. Additionally, state regulators' authority over consumer reporting agencies derives from other regulatory authorities – including responsibility over bank third-party service providers.

On June 25, 2018, state financial regulatory agencies entered into a Consent Order with Equifax Inc., requiring the company to take specific action to protect confidential consumer information in the wake of an extensive

security breach. Equifax, one of the country's three major credit reporting agencies, disclosed in September 2017 that a vulnerability in one of its websites was exploited by criminal hackers in May 2017 to gain access to the personal information of an estimated 146 million U.S. consumers. Data accessed through this cybercrime event included individual customer names, Social Security numbers, birth dates, addresses, and related personally identifiable information.

In response to this breach, a team composed of state financial regulators from Alabama, California, Georgia, Maine, Massachusetts, New York, North Carolina, and Texas initiated a multi-state examination of the company in November 2017 to evaluate the company's information security and cybersecurity controls. The states' examination evaluated the company's cybersecurity, internal audit, risk management, and controls.

In the Consent Order, Equifax agreed to improve how it protects personally identifiable information. The company will restructure its risk management processes, strengthen internal controls and processes, and enhance its oversight by the Board of Directors on the information security program. The corrective actions will apply to Equifax's operations nationwide.
Compliance with the Consent Order will be subject to regulator approval and follow-up reports are required from the company. Additionally, the Consent Order preserves the right of individual states to bring additional actions.

The Consent Order requires the Equifax Board and/or Management to:

- Review and approve a written information security risk assessment.
- Improve the oversight of their audit function by establishing a formal and documented internal audit program that effectively evaluates IT controls.
- Approve a consolidated written Information Security Program and review and an annual report on the adequacy of that program.
- Enhance its oversight of the company's information security program.
- Improve oversight of critical vendors consistent with the guidance from the Federal Financial Institutions Examination Council's (FFIEC) "Outsourcing Technology Services IT Examination Handbook" and "Payment Card Industry Data Security Standards."
- Improve standards and controls for supporting the patch management function and implement an effective patch management program to reduce the number of unpatched systems and instances of extended patching time frames.
- Enhance oversight of disaster recovery and business continuity.
- Submit a list of all remediation projects planned or in process in response to the 2017 breach to the Multi-state Regulatory Agencies.
- Require an independent third party to validate all such remediation projects and provide notice to the Multi-state Regulatory Agencies.
- Provide progress reports on a quarterly basis to the Multi-state Regulatory Agencies.

As part of required ongoing supervision, the company must file written reports with state bank regulators detailing progress with the various provisions of the order on a quarterly basis, and quarterly written progress report submissions will continue until the regulators release the provision.

Cybersecurity

CSBS and its members have a significant focus on and numerous efforts related to cybersecurity, which includes industry outreach, ongoing coordination with federal financial regulatory agencies through state participation in bodies such the Federal Financial Institutions Examination Council (FFIEC) and the Financial and Banking Information Infrastructure Committee (FBIIC), as well as providing state regulators with tools to effectively

supervise institutions for cybersecurity. Last year, CSBS launched a $1.5 million cybersecurity training initiative for state examiners. Additionally, state regulators will roll out new cybersecurity examination procedures in mid-2019 that are applicable to the review of consumer reporting agencies.

GAO Report on Consumer Data Protection

Earlier today, the Government Accountability Office issued a report titled “Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies.” Among GAO’s recommendations is that the Consumer Financial Protection Bureau (CFPB or Bureau) leverage state information or consider registration of consumer reporting agencies to help the CFPB’s monitoring of consumer reporting agencies. State regulators work closely with the Bureau across a broad range of regulatory and supervisory areas and would expect a collaborative and coordinated approach to such an effort.

Amendment to Bank Service Company Act

Moving forward, CSBS encourages enactment of H.R. 241, the Bank Service Company Examination Coordination Act. This legislation will enhance state and federal regulators’ ability to coordinate examinations of and share information on banks’ technology vendors in an effective and efficient manner. Banks partner with third-party service providers (TSPs) to outsource a wide variety of critical banking services. The Bank Service Company Act (BSCA) authorizes federal regulators to examine TSPs to assess the potential risks they pose to individual client banks and the broader banking system. Currently, 38 states have similar authority under state law. The BSCA is silent regarding authorities and/or roles of state banking regulators, limiting the ability of federal and state regulators to share information on TSPs. Amending the BSCA to appropriately reflect state regulators’ authority to examine TSPs will improve state- federal coordination and information sharing and promote more efficient supervision of TSPs that provide critical services to a broad range of banks.

We look forward to working to with the Committee on these issues, and other issues vital to the financial services industry.

Related Posts