protiviti®
Face the Future with Confidence

Compliance Insights

Your monthly compliance news round-up

October
2017

New Cybersecurity Regulation for Financial Services Companies

In March 2017, the New York Department of Financial Services (NYDFS) issued a new regulation regarding cybersecurity for financial services companies (referred to as Part 500). This groundbreaking regulation includes a series of new requirements with tiered deadlines aimed to protect sensitive consumer information and information systems by holding covered entities accountable for their cyber defense responsibilities. Though the requirements are limited to "covered entities" (which includes all banking organizations, insurance companies, money service businesses, and other firms operating in New York under certain state banking, insurance, and financial services laws), all financial institutions – and companies operating outside of financial services – should take note of the requirements of this regulation, chiefly about the development and maintenance of effective cybersecurity programs and annual compliance certification, as it may be applied much more broadly to companies in the future.

The NYDFS established a two-year implementation timeline, outlining the requirements covered entities must meet at designated intervals during this period. While all of the requirements are not effective until March 2019, covered entities will be required to file their first annual compliance certification in February 2018 confirming the proper operation and effectiveness of their cybersecurity programs. The first order of business for covered entities was to establish a cybersecurity compliance framework by August 28, 2017, that includes:

- A designated chief information security officer (CISO) and dedicated, qualified personnel responsible for implementing a cybersecurity program.
- A risk-based cybersecurity program reflecting internal policy on internal and external risk awareness and mitigation.
- Relevant policies and procedures for cybersecurity compliance oversight, reporting, system and network operations, data privacy and monitoring cybersecurity risks.

- Defined user access limits to nonpublic information.
- A documented cybersecurity event incident response plan.
- A defined process for reporting cybersecurity events within 72 hours of discovery.
- Documented self-identified areas, systems or processes requiring material improvement.

Covered entities should be focused on ensuring that they are prepared to certify compliance in February 2018, but importantly should also be preparing for the action items necessary to comply with the March 2018, September 2018 and March 2019 deadlines. Key requirements include:

- A written annual report by the CISO considering the overall effectiveness of the cybersecurity program.
- Risk-based penetration testing and vulnerability assessments.
- A documented, comprehensive, enterprise-wide cybersecurity risk assessment to identify cyber-related vulnerabilities and threats.
- A multi-factor authentication process for data information systems.
- A training program for raising cybersecurity awareness and providing institutional guidance.
- Documented policies and procedures relating to application security, data retention, user access and third-party service providers.
- Controls to ensure audit trails are tracked and retained.
- Encryption of non-public information.

Critical to these efforts is the cybersecurity risk assessment, from which many other elements of the program should be derived. The risk assessment should consider identification, ranking and alignment of assets and associated threats, a mapping of the control environment to potential threats, and an assessment of overall control effectiveness. The assessment should follow the cybersecurity program's policies and procedures, and findings should be integrated into the covered entities' processes for implementing and monitoring cybersecurity program effectiveness. Specific considerations in preparing the risk assessment include:

- Valuation of organization-wide cyber risks facing the financial institution.
- Assessment of internal controls securing and protecting nonpublic information.
- Review of internal record and data management systems for effectiveness of data security.
- Identification of risks and the review of risk management controls.

In preparation for the first annual certification, covered entities should ensure that they have the proper project management in place to support the upcoming certification process. This may include designation of certifiers and potential sub-certifiers, clear delineation of certification-related roles and responsibilities, documented cybersecurity program justification, and communication of key definitions, such as material weaknesses and compensating controls. Further, covered entities may want to consider conducting independent readiness reviews and discussing with their internal audit functions how to help ensure compliance with the regulation and adequacy of the risk assessment in advance of the first certification. Looking towards the upcoming implementation dates, covered entities should also begin prioritizing the completion of the risk assessment to mitigate risk and resolve system vulnerabilities.

CFPB Issues First No-Action Letter Under Project Catalyst Initiative

In September 2017, the Consumer Financial Protection Bureau (CFPB) issued its first no-action letter to a financial technology (fintech) company that proposes to use alternative data in making credit and pricing decisions on consumer loan applications through its online lending platform. This action marks a significant milestone for the CFPB's Project Catalyst, a program initiated in November 2012 that is focused on encouraging marketplace innovation, whereby new financial products and services can be developed in a manner that is consumer-friendly and aligned with Federal consumer financial laws and regulations.

The CFPB introduced the concept of "no-action letters" in 2016 as a mechanism to reduce the regulatory uncertainty associated with new financial products or services. The agency created letter program to facilitate consumer-friendly innovation where regulatory coverage may be unclear for certain new or unreleased financial products or services. Specifically, financial services companies are encouraged to request that the CFPB evaluate a proposed financial product or service and provide either clarification as to how existing laws and regulations might be applied to the product and/or an indication that the agency has no present intention of recommending initiation of an enforcement or supervisory action

against the applicant with respect to the product under applicable laws and regulations. Such letters may be limited in scope to specific facts or circumstances presented by the applicant, and may come with specific requirements and requests by the CFPB of the applicant to enable the agency to monitor effectively the product or service and better inform the agency as to market demand and activity. Applications and the CFPB responses under this program are to be made available to the public by the CFPB.

In the case of this first no-action letter, the company sought guidance from the CFPB regarding its underwriting and pricing model, which is designed to use both traditional lending criteria (e.g., consumer reports and credit scores from nationwide consumer reporting agencies) and so-called "alternative" criteria (e.g., education levels and type, employment, etc.) to underwrite loan applications and extend credit to consumers. In particular, the company indicated that its use of alternative data and underwriting techniques enables it to evaluate better the credit risk of consumers with limited credit histories, providing expanded credit access to these consumers at comparatively lower costs. In its application, the company identified, however, that regulatory uncertainty related to compliance with the Equal Credit Opportunity Act (ECOA, as implemented by the CFPB's Regulation B) hindered its ability to develop and expand products, and that further clarity and assurances from the CFPB would be beneficial.

In the CFPB's letter issued to the company, the agency indicates that it had no present intent to initiate supervisory or enforcement action against the company related to the ECOA. Significant points related to the letter include:

- The CFPB requires regular reporting by the company of lending and compliance information to the agency as a condition of the no-action letter.
- The letter applies exclusively to the application of Regulation B to the company's automated model for underwriting applicants for unsecured non-revolving credit.
- The letter is limited in use as detailed by the requirements the company set forth in its request and compliance plan submitted at the time of application. Modifications or revocation of the letter can occur at any time and at the discretion of the CFPB staff.
- The letter is non-binding, should not be viewed as a waiver or safe harbor, and can be modified or revoked by the CFPB at any time for any reason.

The company also committed in its request to the CFPB to continuously share fair lending and access-to-credit test results with the agency, and is required to notify the CFPB whenever additional factors are implemented to its underwriting model.

The no-action letter highlights the CFPB's dedication to encouraging financial innovation, particularly where new products and services and alternative methods can provide underserved consumers with increased access to credit. Though the process to obtain such a letter involves public disclosure and potentially additional requirements imposed by the CFPB on an applicant, the benefits to financial services companies are significant in terms of providing clarity on regulatory expectations. Financial services companies that are developing innovative consumer financial products and services should explore the pros and cons associated with obtaining a no-action letter and partnering with the regulatory agencies as part of its new products/services development strategy.

CFPB Amends Regulation B to Align With Forthcoming Changes to HMDA Data Collection and Reporting Requirements

In September 2017, the CFPB issued a final rule amending and clarifying certain provisions of its Regulation B (which implements the ECOA) regarding the ability of lenders to collect and retain certain demographic information from home mortgage applicants. These changes are being made to synchronize the Regulation B requirements with the revisions to the CFPB's Regulation C (which implements the Home Mortgage Disclosure Act, or HMDA) effective in January 2018, and to permit greater flexibility to mortgage lenders in collecting this information.

In general, Regulation B prohibits a creditor from inquiring about certain applicant characteristics (e.g., race, color, religion, national origin and sex), except for limited circumstances, in particular for applications for credit primarily for the purchase or refinancing of an applicant's principal dwelling, or as otherwise required by law, regulation or order. Regulation C is an example of the latter situation, as it explicitly requires mortgage lenders to collect specific data elements (in particular, race, ethnicity and sex) for certain dwelling-secured loans. In addition, the types of dwelling-secured loans under Regulation C that requires the collection of these data elements in a more expansive way than permitted under Regulation B. The CFPB recognizes that certain lenders may not be subject to Regulation C reporting requirements, or may seek to voluntarily collect demographic information on certain loan types that are otherwise exempt from Regulation C reporting requirements but for which the lender seeks to optionally report, so as to maintain consistent compliance standards. The revisions implemented by this final rule provide flexibility for lenders in these cases to engage in this data collection and reporting without violating Regulation B.

In addition, the final rule will allow creditors to collect information regarding an applicant's ethnicity and race using the more expansive race and ethnicity subcategories that financial institutions subject to Regulation C will be required to use. Under Regulation C, lenders will be required to allow applicants to self-identify using more expansive, "disaggregated" race and ethnicity subcategories (e.g., Mexican, Puerto Rican, Cuban) rather than the current "aggregated" categories (e.g., Hispanic or Latino). The CFPB stops short of requiring lenders not subject to Regulation C to use the disaggregated categories, recognizing that such lenders could find the requirements more burdensome; lenders subject to Regulation C are otherwise minimally impacted by this change. The CFPB does allow creditors not subject to Regulation C to choose, on an application-by-application basis, whether to collect information using the disaggregated or aggregated categories. It should be noted, however, that a creditor is not permitted to collect disaggregated data on the basis of visual observation; if not provided voluntarily by the applicant the creditor may only document race and ethnicity information at the aggregate level.

Finally, the CFPB eliminates the 2004 Uniform Residential Loan Application (URLA) in the appendix to Regulation B as a model form for how demographic information about applicants should be collected, as it has become outdated, replacing it with two model forms – one each for collection of aggregated or disaggregated data.

Mortgage lenders, in particular those not subject to Regulation C reporting requirements, should evaluate the changes to Regulation B and understand how these changes by the CFPB will impact existing operational practices and mortgage loan origination platforms. Where a mortgage lender seeks to collect demographic information otherwise not required by Regulation C, the lender should evaluate with its compliance and legal personnel the Regulation B changes for permissibility. All mortgage lenders should be aware of implementation resources made available by the CFPB regarding Regulations B and C, and incorporate these tools, guides and other materials into their implementation plans.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®