EY
Building a better working world

Cybersecurity requirements for financial services companies

Overview of the finalized Cybersecurity Requirements from the New York State Department of Financial Services (DFS)

February 2017

Overview

This document provides a summary of the finalized NY DFS Cybersecurity Requirements announced on February 16, 2017.

The New York State Department of Financial Services (DFS) has become increasingly concerned about the number of cybersecurity events affecting DFS-regulated financial services firms, as well as the potential risks posed to the industry at large. On September 28, 2016, NY DFS proposed new requirements relating to cybersecurity for all DFS-regulated entities. As a result of the feedback received, the NY DFS released a new revised proposal of cybersecurity requirements as of December 28, 2016. On February 16, 2017, the finalized NY DFS cybersecurity requirements (23 NYCRR 500) were posted to the New York State Register, and they will take effect on March 1, 2017. On an annual basis, firms will be required to prepare and submit to the superintendent a Certification of Compliance with the NY DFS Cybersecurity Regulations commencing February 15, 2018. While the finalized requirements are somewhat less arduous, many affected institutions will still have challenges to implement an effective program within the required timelines.

The finalized requirements include areas such as:

- **Definitions:** The finalized requirements include definitions for organizations such as risk assessment, risk-based authentication, third parties and a modified definition for Nonpublic Information (NPI).
- **Cybersecurity program and policy:** Firms should adopt an approved, written cybersecurity policy and supporting policies and procedures to protect their Information Systems and NPI. The program should enable the firm to:
  - Identify cyber risks
  - Protect against unauthorized access/ use or other malicious acts
  - Detect cybersecurity events
  - Respond to identified cybersecurity events to mitigate any negative events
  - Recover from cybersecurity events and restore normal operations and services

Notice posted to New York State Register
- February 16, 2017

Effective date
- March 1, 2017

Transition period
- 180 days after effective date

Entities covered
- Operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking, insurance or financial services law

Exemptions criteria
- Fewer than 10 employees, including independent contractors are the firm's Affiliates located in NY or responsible for the business of the firm
- Less than $5m in gross revenue each of last three fiscal years from NY business operations
- Less than $10m in year-end total assets is calculated in accordance with generally accepted accounting principles, including assets of all Affiliates

Overview (cont.)

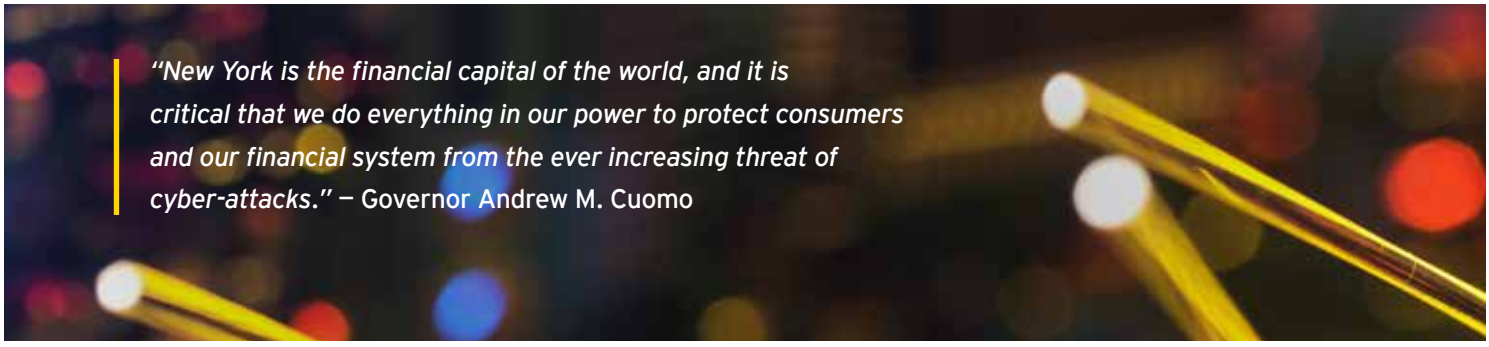
- **Risk assessment, testing and compliance:** Firms should rigorously assess the risks associated with their Information Systems. A firm's risk assessment will be utilized to provide the basis for how it addresses requirements under the finalized DFS requirements. On an annual basis, firms should conduct penetration testing, and vulnerability assessments should be performed biannually, both of which are based on the firm's risk assessment.
- **Personnel, resources and training:** Firms should designate a qualified chief information security officer (CISO) to drive the cybersecurity program. More broadly, in light of these finalized requirements, firms should validate that they have the necessary resources (in-house or from a third party) to meet their new cyber responsibilities, and that employees have the necessary training.
- **Access privileges, application security and NPI encryption:** Firms need robust policies and procedures to address these issues. NPI should be encrypted; where compensating controls are used instead, they must be approved by the CISO.
- **Audit and NPI records retention:** Firms need rigorous systems, policies and procedures to provide for a holistic audit trail. NPI should be destroyed appropriately.
- **Third parties:** Firms need to validate that third parties are capable of adhering to new cyber requirements and implement contractual terms to enforce these requirements.
- **Incident response and notification:** Firms should adopt robust incident management plans and should be able to notify the DFS of material events within 72 hours.

Definition of Information Systems: A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems

Definition of Nonpublic Information: Nonpublic Information (NPI) is defined as all electronic information that is not publicly available information and is:

- Business-related information
- Information concerning an individual, which, because of name, number, personal mark or other identifier, can be used to identify such an individual when combined with SSN, driver's license, account number, security code or biometric records
- Any information or data, except age or gender, obtained from a health care provider that relates to an individual's past, present or future physical or mental behavior for an individual or their family, including the provision of health care, and the payment for the provision of health care

Definition of Third Party Service Provider(s): Third Party Service Provider(s) (third party or third parties) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.



Overall program and policy framework

Firms should establish and maintain an enterprise-wide cybersecurity program and policy that enable them to identify, measure, manage and mitigate cyber risks.

Cybersecurity program

- Each firm shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of its Information System. The program shall be based on the entity's risk assessment and designed to perform the following core cybersecurity functions:
  - Identify and assess internal and external cyber risks that may threaten the security or integrity of NPI stored on the entity's Information System
  - Use defensive infrastructure
  - Implement policies and procedures to protect the firm's Information Systems, and NPI stored on those systems, from unauthorized access, use or other malicious acts
  - Detect cybersecurity events
  - Respond to identified or detected cybersecurity events to mitigate any negative effects
  - Recover from cybersecurity events and restore normal operations and services
  - Fulfill applicable regulatory reporting obligations

Cybersecurity policy

- Each firm shall implement and maintain a written cybersecurity policy approved by a Senior Officer or board of directors that sets out procedures to protect its Information Systems and NPI stored on those Information Systems. The cybersecurity policy shall be based on the entity's risk assessment and address the following:
  - Information security
  - Data governance and classification
  - Asset inventory and device management
  - Access controls and identity management
  - Business continuity and disaster recovery planning and resources
  - Systems operations and availability concerns
  - Systems and network security
  - Systems and network monitoring
  - Systems and application development and quality assurance
  - Physical security and environmental controls
  - Customer data privacy
  - Vendor and Third Party Service Provider management
  - Risk assessment
  - Incident response

Modifications from original proposal

- Added that documentation related to a firm's cybersecurity program be available for inspection by the superintendent upon request
- Updated that the firm's cybersecurity policy to be based upon its risk assessment
- Added that the asset inventory and device management program be included in a firm's cybersecurity policy
- Modified that the cybersecurity policy be approved by the CISO instead of the board of directors

Implications

- Firms should evaluate their overall NPI definition to validate that they are in alignment with the NPI requirements.
- Firms should review their overall cybersecurity programs and create a repository to document their enterprise-level cybersecurity policy to determine that they cover the identified areas and maintain supporting program documentation.
- Firms should benchmark their standards, policies and procedures against industry practices.

Risk assessment, testing and compliance

Firms should formally evaluate their cyber risks and the effectiveness of the related controls. Firms' systems and applications should be assessed routinely.

Risk assessment

- Each entity shall conduct a periodic risk assessment of its Information Systems sufficient to inform the design of the cybersecurity program. The risk assessment shall be updated as necessary to address changes to the entity's Information Systems, NPI or business operations. The risk assessment shall allow for the revision of controls to respond to technological developments and evolving threats, and shall consider the risks of its business operations related to cybersecurity, NPI collected or stored, Information Systems utilized, and the availability and effectiveness of controls to protect NPI and Information Systems. The risk assessment shall be carried out in accordance with written policies and processes and shall be documented, including:
  - Criteria for evaluating and categorizing identified cybersecurity risk or threats facing the firm
  - Criteria for assessing the confidentiality, integrity, security and availability of the firm's Information Systems and NPI, including the adequacy of existing controls in the context of identified risks
  - Requirements for describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks

Penetration testing and monitoring

- The cybersecurity program for the entity shall include monitoring and testing, developed in accordance with the entity's risk assessment, which is designed to assess the effectiveness of the firm's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments.

Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, firms shall conduct:

- Annual penetration testing of the firm's Information System based on relevant risks identified in accordance with the risk assessment
- Biannual vulnerability assessments, including systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities
- Implementation of risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, NPI by such Authorized Users

Annual compliance representation

- Annually, each entity shall submit to the superintendent a written statement covering the prior calendar year by February 15, certifying that the entity is in compliance with the requirements set forth. Each firm shall maintain for an examination by the NY DFS all records, schedules and data supporting this certification for a period of five years. If a firm has identified areas, systems or processes that require material improvement, updating or design, the firm shall document the identification and remedial efforts planned and underway. This documentation must be available for inspection by the superintendent.

Modifications from original proposal

- The risk assessment process was modified from an annual process to a periodic one and should include sufficient information to assess the design of the firm's cybersecurity program as defined by the NY DFS cybersecurity requirements.
- Monitoring and vulnerability/penetration testing was modified to continuous and/or periodic based on the firm's risk assessment.
- The due date for the written statement to the superintendent regarding compliance with the NY DFS cybersecurity requirements was modified to February 15 of each year and clarified that the period covered by the certification was the prior year.

Implications

- Firms should review their cyber risk assessment approach to validate that it effectively evaluates the evolving cyber risks facing the firm, as well as the effectiveness of its cyber risk controls to address identified risks, and that it promotes prompt and thorough remedial action, when required.
- Firms should evaluate the frequency and effectiveness of their penetration testing and vulnerability assessment strategy and techniques.

Personnel, resources and training

Firms should appoint a strong cybersecurity leader and verify they have the right people, resources and firmwide cybersecurity training.

Chief information security officer (CISO)

- Each firm shall designate a qualified individual to serve as the CISO, who is responsible for implementing, overseeing and enforcing the firm's cybersecurity program and policy.
- At least annually, the CISO shall report to the board of directors or governing body in writing on the firm's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:
  - The confidentiality of NPI and the integrity and security of the firm's Information Systems
  - The firm's cybersecurity policies and procedures
  - The firm's material cyber risks
  - The overall effectiveness of the firm's cybersecurity program
  - Material cybersecurity events that affected the firm during the time period addressed by the report

Personnel and resources

- Each firm should utilize qualified cybersecurity personnel, an Affiliate or Third Party Service Provider sufficient to manage its cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions outlined in its cybersecurity program.

Training

- Each firm shall:
  - Provide cybersecurity personnel with cybersecurity update and training sessions sufficient to address relevant cybersecurity risks
  - Verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures
  - Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the firm in its risk assessment

Modifications from original proposal

- Modified the requirements so that the CISO may now be employed at the organization or a third-party service provider
- Changed the CISO's requirement for reporting to the board of directors to be on an annual basis and in writing
- Updated the CISO's reporting requirements to the board of directors to focus on material cyber events instead of all cyber events
- Updated the training requirements to be based on risk scenarios identified as part of the risk assessment process

Implications

- Firms should assess their cybersecurity organizational structure and determine the appropriate placement and reporting lines of the CISO. Special attention should be paid to the independence of the CISO. Firms may need to revise roles and responsibilities across the first and second lines of defense.
- Firms should reassess their resource and personnel needs in light of the new requirements and should review and potentially enhance periodic and ongoing cybersecurity training provided to personnel.

Access, application security and encryption

Firms should effectively manage access and application security and should encrypt NPI or develop plans to be able to do so.

Access privileges and authentication

- **Access privileges:** A firm's cybersecurity program based on its risk assessment shall limit user access privileges to Information Systems that provide user access to NPI and shall periodically review such access privileges.
- **Multifactor authentication (MFA):** Based on its risk assessment, each firm shall use effective controls, which may include MFA or Risk-Based Authentication to protect against unauthorized access to NPI or Information Systems. MFA shall be utilized for any individual accessing the firm's internal networks from an external network, unless the firm's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Application security

- A firm's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house-developed applications utilized by the firm, and procedures for evaluating, assessing or testing the security of externally developed applications utilized within the firm's technology environment.
  - All procedures, guidelines and standards shall be periodically reviewed, assessed and updated as needed by the CISO (or qualified designee) of the firm.

Encryption of NPI

- As part of a firm's cybersecurity program and based on its Risk Assessment, it shall implement controls that include encryption to protect NPI held or transmitted by the firm both in transit over external networks and at rest.
  - If the firm determines that encryption of NPI in transit over an external network is not feasible, the firm may instead secure NPI using effective alternative compensating controls reviewed and approved by the firm's CISO.
  - If the firm determines that encryption of NPI at rest is not feasible, the firm may instead secure NPI using effective alternative compensating controls reviewed and approved by the firm's CISO.
  - To the extent that the entity is utilizing compensating controls for the encryption of NPI, the feasibility of the encryption and the effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Modifications from original proposal

- A review of application security procedures, guidelines and standards was modified from an annual review by the CISO to a periodic review.
- Multifactor authentication was modified from specific types of access to the entity determining what its critical assets and access paths are based upon its risk assessment to protect against unauthorized access to NPI.
- The finalized requirements permit the CISO to approve in writing the use of reasonably equivalent or more secure access controls in lieu of MFA.
- Encryption requirements have been updated based upon what is feasible or not feasible for an organization by identifying alternative compensating controls that have been reviewed and approved by the firm's CISO at least annually.

Implications

- Firms should review their access privileges and authentication approach – and those related to application security – to validate they meet the new standards and are in line with industry practices.
- Firms should review their approach to NPI encryption, and to the extent they will be relying on compensating controls in lieu of encryption, they should work with their CISO to develop a transition plan to phase out these controls.
- Firms should consider their secure development practices as well as testing of externally developed applications for security measures.

Audit trail and NPI record destruction

Firms should implement rigorous processes and procedures to provide for a broad audit trail of activities, as well as effective processes to destroy NPI.

Audit trail

- Each firm shall securely maintain systems that, to the extent applicable and based on its risk assessment:
  - Are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the firm. Each firm shall maintain these records for not fewer than five years.
  - Include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations for the firm. Each firm shall maintain these records for not fewer than three years.

Limitations on data retention

- As part of its cybersecurity program, each firm shall include policies and procedures for the secure disposal on a periodic basis of any NPI that is no longer necessary for business operations or for other business purposes, except where such information is required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Modifications from original proposal

- Audit trails were modified to focus on the information an organization needs to reconstruct material transactions and support the operations of the firm.
- The time frame to maintain audit trails to reconstruct material financial transactions was modified to at least five years.
- The time frame to maintain audit trails designed to detect and respond to Cybersecurity Events was modified to at least three years.

Implications

- Firms should review and, where necessary, enhance their capabilities — systems, processes and policies — to meet the audit trail requirements set out by the DFS.
- Firms should review their document retention policies and procedures relating to NPI, taking into account industry practice on what constitutes timely and effective destruction of NPI.

Third parties

Firms should implement rigorous third-party cybersecurity risk management policies and procedures across the full life cycle of the relationship with the third parties.

Third parties

- Each firm shall implement a written policies and procedures designed to ensure the security of Information Systems and NPI that are accessible to or held by third parties. Such policies and procedures shall be based on the Risk Assessment of the firm and shall be addressed to the extent applicable:
  - Identification and risk assessment of third parties to service providers
  - Minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the firm
  - Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers
  - Periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices
- Such policies and procedures shall include guidelines for due diligence and/or contractual protections related to Third Party Service Providers, including to the extent applicable guidelines addressing:
  - The Third Party Service Provider's policies and procedures for access controls, including its use of MFA to limit access to relevant Information Systems and NPI
  - The Third Party Service Provider's policies and procedures for the use of encryption to protect NPI in transit and at rest
  - A notice to be provided to the firm in the event of a Cybersecurity Event directly impacting the firm's Information Systems or NPI being held by the Third Party Service Provider
  - Representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the firm's Information Systems or NPI

Modifications from original proposal

- Assessments of third parties was modified from annual to periodic and is based upon the risk they present.
- The requirement of a firm to perform a cybersecurity audit of a third party was removed.
- The finalized requirement added a new limited exception that an agent, employee, representative or designee of the covered entity, who is himself or herself a covered entity, does not need to develop its own third-party information security policy if the agent, employee, representative or designee covers the policy of the covered entity.

Implications

- Firms should review their third-party/vendor risk management standards, policies and procedures to verify they meet the new requirements; this should include evaluating the manner and frequency with which they conduct off-site and on-site cybersecurity assessments of third parties.
- Firms should review their procurement/contracting process – and standard terms for third parties – to validate that all of the necessary new provisions are covered.
- Firms should determine how to implement these standards for existing, as well as new, third parties.

Incident response and notifications

Firms should put effective incident response programs in place, as well as effective mechanisms to notify the DFS of material cyber events.

Incident response

- A firm's cybersecurity program shall establish a written incident response plan designed to promptly respond to and recover from any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the firm's Information Systems or the continuing functionality of any aspect of the firm's business or operations.
- Such incident response plan shall address:
  - Internal processes for responding to a Cybersecurity Event
  - Goals of the incident response plan
  - The definition of clear roles, responsibilities and levels of decision-making authority
  - External and internal communications and information sharing
  - Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls
  - Documentation and reporting regarding Cybersecurity Events and related incident response activities
  - Evaluation and revision of the incident response plan following a Cybersecurity Event

Notifications to DFS

- Each firm shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occured that is either of the following:
  - Cybersecurity events of which notice is required to be provided to any government body, self-regulatory agency or other supervisory body; or
  - Cybersecurity events that have a reasonable likelihood of harming any material part of the normal operations of the firm

Modifications from original proposal

- The finallized requirement added the word "materially" for incidents and events that impact a firm.
- The requirement to notify the superintendent was changed such that firms must notify the superintendent if either Cybersecurity Event Scenario occurs.
- The time frame of 72 hours to report a cyber incident remains unchanged.

Implications

- Firms should reevaluate their incident response plans to validate that they meet the new requirements; this includes determining the manner in which plans are enhanced, as required, after incidents have occurred – that is, that an effective feedback loop is in place.
- Firms should validate that their reporting protocols would provide for timely notification of matters to the DFS and, before that, provide for appropriate escalation within the company to senior management and, where necessary, the board of directors.

Immediate actions

Firms should evaluate the potential range of changes that may be required to their cybersecurity approach and discuss these with senior management, the CISO and the board of directors.

- Review the DFS requirements and evaluate the range of potential changes that would be needed to your:
  - Cybersecurity program and policies and risk assessment process
  - Penetration testing and vulnerability assessment approach
  - Policies and procedures related to access privileges, authentication, application security and encryption
  - Third-party risk management policy and procedures
  - Incident response
  - Cybersecurity organization and personnel strategy and structure, along with cybersecurity training
- Brief your board of directors and executive management on the DFS requirements and their potential implications to your organization
- Consider how other regulatory requirements and proposals — e.g., the October 19, 2016, advanced notice of proposed rulemaking from the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Federal Reserve Board — may influence the manner in which your firm implements the DFS cybersecurity requirements

EY contacts

William Beer
+1 212 360 9010
william.beer@ey.com

Chris Lanzilotta
+1 410 783 3739
christopher.lanzilotta@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

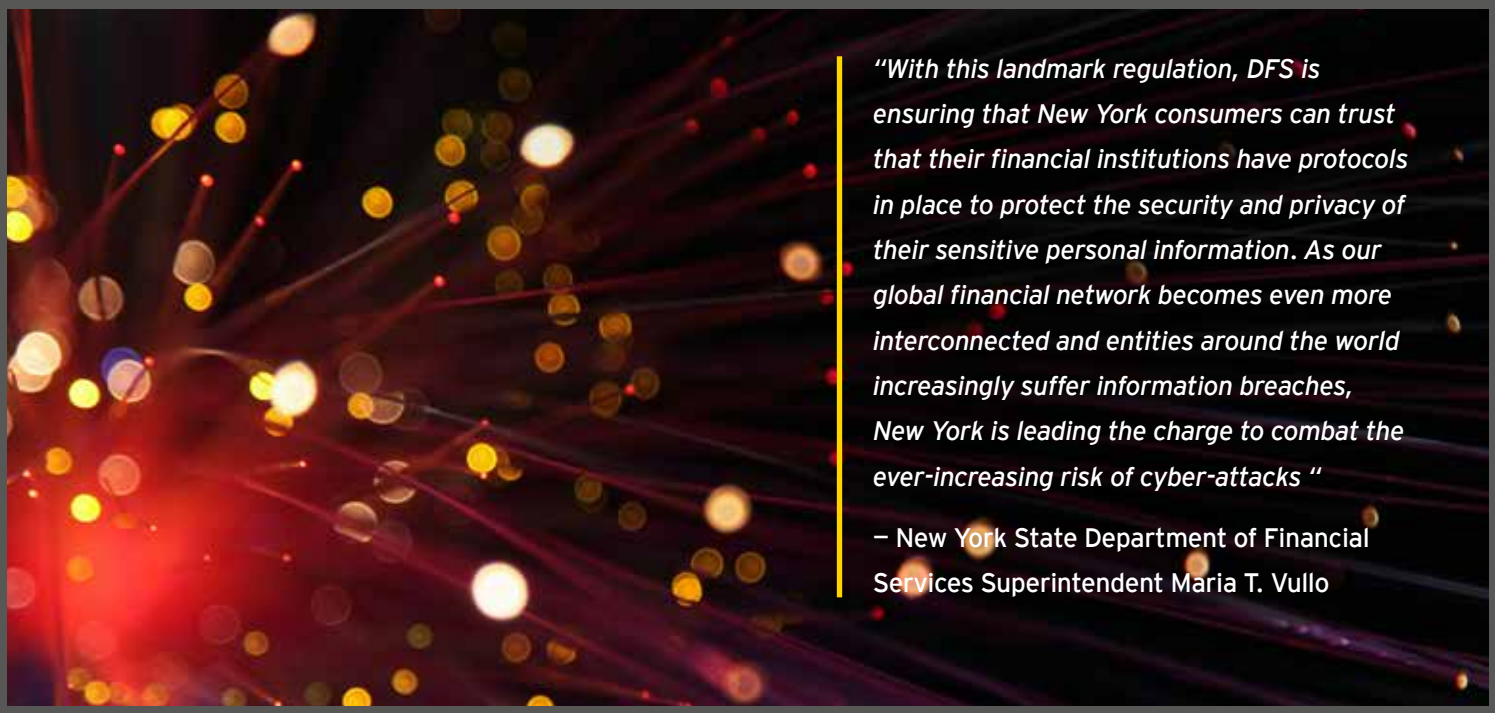
Ertem Osmanoglu
+1 212 773 3520
ertem.osmanoglu@ey.com

Jaime Kahan
+1 212 773 7755
jaime.kahan@ey.com

JB Rambaud
+1 212 773 4617
jb.rambaud@ey.com

Chris Kipphut
+1 704 338 0491
chris.kipphut1@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com



"With this landmark regulation, DFS is ensuring that New York consumers can trust that their financial institutions have protocols in place to protect the security and privacy of their sensitive personal information. As our global financial network becomes even more interconnected and entities around the world increasingly suffer information breaches, New York is leading the charge to combat the ever-increasing risk of cyber-attacks "

– New York State Department of Financial Services Superintendent Maria T. Vullo

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

SCORE No. 00841-171US
1702-2198774 BDFSO
ED None

ey.com