New York Releases Proposed Cybersecurity Regulations Affecting Banks, Insurers and Other Financial Services Firms

The New York State Department of Financial Services ("DFS") on September 13, 2016, proposed regulations that would mandate cybersecurity standards for any entity authorized by DFS to operate in New York, including certain banks and insurance companies doing business in New York. The proposed regulations, titled "Cybersecurity Requirements for Financial Services Companies" ("Proposed Regulations"), would expand upon the areas discussed as potential areas for regulation in DFS's November 9, 2015, letter to the Financial and Banking Information Infrastructure Committee, a coordinating body comprised of the key federal and state banking, insurance and securities regulatory agencies ("FBIIC Letter").[1] (See our November 23, 2015, Legal Update for an analysis of the FBIIC Letter.) Once published in the New York State Register, the Proposed Regulations will be open for a 45-day public comment period.[2]

The intent of the Proposed Regulations, as expressed by DFS in the preamble, is to "promote the protection of customer information as well as the information technology systems of regulated entities," whether controlled by the entities themselves or by external service providers. Acknowledging that the "number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark," the Proposed Regulations explicitly state that cybersecurity is a "priority for New York State."

This Legal Update is divided into three parts, which (i) describe the entities affected by the Proposed Regulations, (ii) provide an explanation of the substantive requirements of the Proposed Regulations and (iii) discuss the implications of the Proposed Regulations for the broader financial services industry.

Who Would Be Affected by the Proposed Regulations?

The Proposed Regulations would apply to any person or entity "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" under the New York banking, insurance or financial services laws (i.e., any entity subject to the authority of DFS) (each, a "Covered Entity").[3] Because the Proposed Regulations would require that a Covered Entity ensure that its third-party service providers ("TSPs") implement policies and procedures designed to ensure the security of the Covered Entity's systems and data, the Proposed Regulations have the potential to become a new *de facto* standard for the broader national insurance and financial services industry, especially if other states issue similar rules. Banks and insurance companies without any regulatory connection to DFS (e.g., banks without licensed or registered offices or branches in New York and "49 state" insurance companies) generally would not be covered by the Proposed Regulations, although bank and

insurance company-affiliated service providers that provide services to an affiliated Covered Entity would likely be included under the TSP provision of the Proposed Regulations.

Any Covered Entity with (i) fewer than 1,000 customers in each of the preceding three calendar years, (ii) less than $5 million in gross revenue in each of its preceding three fiscal years and (iii) less than $10 million in year-end total assets (when aggregated with its affiliates), would be exempted from the CISO, penetration and vulnerability testing, auditability, application development, cybersecurity personnel, multi-factor authentication, training, encryption and incident response plan requirements of the Proposed Regulations.

Subject to a 180-day transition period for most provisions, the Proposed Regulations would become fully effective on January 1, 2017, for Covered Entities not able to avail themselves of the *de minimis* exemption. If a Covered Entity ceases to qualify for this *de minimis* exemption, it would have 180 days from the end of its fiscal year to comply with all requirements of the final regulations.

The Proposed Regulations

Under the Proposed Regulations, each Covered Entity would be required to implement a program "designed to ensure the confidentiality, integrity and availability" of its information systems and data, with particular reference to (i) nonpublic information ("NPI") in its possession (a category defined to include not only personally identifiable information but also other business information whose revelation would cause a material adverse impact to a Covered Entity's business and operations), (ii) preventing, detecting, responding to and mitigating the effects of breaches of its information systems and (iii) fulfilling all regulatory reporting obligations. Information systems are broadly defined as including most electronic information resources, as well as specialized systems such as telephone exchanges and environmental controls.

Written Policies and Procedures. A Covered Entity would be required to implement its cybersecurity program through written policies and procedures, and such policies and procedures would need to be periodically (and at least annually) (i) reviewed by a Covered Entity's board and (ii) approved by a senior officer or committee responsible for the management, operations, security, information systems, compliance and/or risk management of the Covered Entity. At a minimum, such policies and procedures would need to address:

- Information security;
- Data governance and classification;
- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Capacity and performance planning;
- Systems operations and availability concerns;
- Systems and network security and 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; and
- Incident response.

Chief Information Security Officer, Governance, Annual Certification. A Covered Entity would need to designate a Chief Information Security Officer ("CISO"), who would be responsible for overseeing and implementing the Covered Entity's cybersecurity program and who would provide a report to the Covered Entity's board or other governing body at least bi-annually, assessing compliance with its cybersecurity program, identifying breaches and deficiencies and proposing remediation.

Certain CISO functions may be outsourced, but a Covered Entity nevertheless would remain responsible for complying with the Proposed Regulations.

The board (or one of the senior officers of the Covered Entity) in turn would need to certify the Covered Entity's compliance with the Proposed Regulations to DFS on an annual basis by January 15 of each year beginning in 2018. To the extent that a Covered Entity identifies areas of needed improvement, the certification would need to address these areas and planned remediation. All of the materials supporting the certification would need to be maintained for five years and made available for inspection by DFS.

Testing and Risk Assessment. Each Covered Entity would be required to conduct annual penetration testing and quarterly vulnerability assessments to gauge the effectiveness of its cybersecurity program and to conduct an annual risk assessment of its information systems with results documented in writing. Any "material risk of imminent harm" relating to a Covered Entity's cybersecurity plan would need to be communicated to DFS within 72 hours of discovery and subsequently disclosed in the annual certification described above.

Personnel and Training. A Covered Entity would be required to employ cybersecurity personnel sufficient to maintain and execute the Covered Entity's cybersecurity program. The personnel would be subject to continuing education requirements, but all of a Covered Entity's personnel would need to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified in its annual risk assessment (discussed above). Covered Entities would also be required to implement risk-based monitoring of authorized users of its systems, as well as controls designed to detect unauthorized access to or use of, or tampering with, NPI by authorized users.

Audit Trail. A cybersecurity program would need to include the ability to audit (i) privileged user access to critical systems, (ii) any alteration of or tampering with hardware systems (including through the use of physical access controls and event logs) or data; and (iii) system events, including accessing, altering or tampering with the audit system itself. While the above audit trail system requirements were detailed in the FBIIC Letter, the Proposed Regulations would extend the audit requirement to include a six-year audit records retention requirement and, notably, the ability to completely and accurately reconstruct all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a breach. (Notwithstanding the above retention requirement, the Proposed Regulations also would mandate the timely destruction of outdated or obsolete NPI whose retention is not required by law or regulation.) In addition, a Covered Entity would need to limit access to NPI stored on its systems to those with a "need to know."

In-house Software Development. The FBIIC Letter signaled that the standards would mandate secure development practices for in-house developed software applications (to minimize zero-day attacks), which would be reviewed by the CISO and updated at least annually; the Proposed Regulations include these concepts without modification.

Multi-factor Authentication. The Proposed Regulations would mandate the use of multi-factor authentication methods (e.g., password and token or text messaging code) for individuals accessing the Covered Entity's internal systems or data from an external network and for privileged access to database servers holding NPI. In addition, risk-based authentication (requiring additional verification, such as the use of challenge questions, when anomalies or changes in normal use patterns of a user are detected) would be required for web applications that capture, display or interface

with NPI, and such web applications would also be required to support multi-factor authentication.

Encryption of NPI. All NPI stored or transmitted by a Covered Entity would need to be encrypted, though the Proposed Regulations would provide that where encryption is currently infeasible, appropriate alternative compensating controls reviewed and approved by the CISO may be used for not longer than one year (in the case of NPI in transit) or five years (in the case of stored NPI) after the effective date of the Proposed Regulations.

Incident Response Plans. Written incident response plans, documenting a Covered Entity's ability to promptly respond to and recover from a breach affecting its systems or data, would need to be put in place, addressing, at a minimum, the goals of the incident response plan and internal processes for responding to a breach, including:

- Clearly defined roles, responsibilities and levels of decision-making authority;
- External and internal communications plans and information sharing;
- Remediation of identified weaknesses;
- Documentation and reporting of breaches and related incident response activities; and
- Evaluation and revision of the incident response plan following a breach.

Breach Notification. Covered Entities would be required to notify DFS within 72 hours after becoming aware of any breach with a "reasonable likelihood of materially affecting the normal operation of the Covered Entity or that" affected NPI, including but not limited to a breach of which notice is provided to any government or self-regulatory agency or involving actual or potential tampering with, or unauthorized access to or use of, NPI. While not expressly stated, the Proposed Regulations imply that Covered Entities also will be required to provide identity protection services to customers impacted by a breach.

Third-Party Service Providers. Concern about the potential use of TSPs as a potential point of entry for hackers continues to be an area of particular concern for DFS. The Proposed Regulations therefore would overlay on TSPs most of the provisions applicable to Covered Entities by directing Covered Entities to develop written policies and procedures designed to ensure security of systems and data accessible to, or held by, TSPs. (It is not clear at this stage whether the intent is for intercompany "shared services" arrangements to be covered by these provisions. If so, financial services groups that contain Covered Entities subject to the Proposed Regulations may be forced to apply the DFS cybersecurity standards on a groupwide basis or, alternatively, bear the increased costs which would result from maintaining staff and hardware to support parallel systems.)

Covered Entities would be expected to perform a risk assessment on their TSPs and conduct initial due diligence on, and annual assessments of, their TSPs' cybersecurity practices. TSPs would be required to meet minimum cybersecurity standards in order to do business with Covered Entities. Additionally, each Covered Entity would be required to establish "preferred provisions" for service contracts with their TSPs addressing (i) the use of multi-factor authentication, (ii) encryption of NPI in transit and at rest, (iii) prompt breach notification to the Covered Entity, (iv) audit of the TSPs' cybersecurity measures, (v) the provision of identity protection services to the Covered Entity's customers materially impacted by a breach resulting from the TSPs' negligence or willful misconduct and (vi) representations and warranties from the TSPs concerning the safety and security of their systems accessing or interacting with the Covered Entity's systems and NPI.

Implications for Affected Industries

Insurance. The Proposed Regulations would apply to natural persons and business entities that are licensed or authorized by DFS, including insurance companies, insurance agents and brokers and insurance adjusters. It does not appear that the Proposed Regulations would apply to (i) nonadmitted insurers that insure New York risks on an excess and surplus line basis or (ii) nonadmitted reinsurers that provide reinsurance to New York cedents or with respect to New York risks. However, the excess line brokers and reinsurance intermediaries who place risks with such insurers and reinsurers would be Covered Entities, and there could be some indirect impact on nonadmitted companies by virtue of their transactions with such brokers and intermediaries or their affiliate relationships.

By virtue of the McCarran Ferguson Act, the business of insurance is primarily regulated at the state rather than federal level, although the National Association of Insurance Commissioners ("NAIC") endeavors to foster a measure of uniformity across the states through the development of model laws and regulations. It is important to note, therefore, that DFS's initiative in announcing the Proposed Regulations at the present time has occurred against the backdrop of a parallel effort by the NAIC's Cybersecurity Task Force to develop an Insurance Data Security Model Law. It now appears that New York may be overtaking the NAIC on this issue. Furthermore, it is hard to imagine that the NAIC's Cybersecurity Task Force will be able to move forward on its model law drafting project without at least taking account of the DFS proposals. It is also possible that stakeholders might view the Proposed Regulations as a nascent *de facto* national standard once in effect.

The Proposed Regulations would impact different segments of the insurance industry differently. Because of the nature of their business and of the data they collect, property/casualty insurers have not traditionally been subjected to the same level of regulatory scrutiny in this area as life and health insurers, who must comply with data security standards under a number of federal laws such as HIPAA. Many insurance agents and brokers are small businesses, and it is unclear whether the *de minimis* exception has been sufficiently tailored to exclude, for instance, an independent agent who may be well under the revenue and asset thresholds but have over 1,000 customers. Associations representing smaller agents and brokers may wish to seek further expansion of the *de minimis* exception during the comment period.

Banking. As noted above, the Proposed Regulations would apply to all banking organizations regulated by DFS, including all New York-chartered banks, trust companies, and credit unions, and New York-licensed branches, agencies, and representative offices of non-US banks. The Proposed Regulations may even cover several categories of banking organizations that are not typically subject to prudential regulation by DFS, such as (i) national banks and non-New York-chartered state banks that have registered with DFS to operate a branch or domestic representative office in New York; and (ii) bank holding companies that own two or more state or national banks located in New York. These banking organizations may use the comment period to request clarification from DFS as to the coverage of the Proposed Regulations and their interplay with federal laws, such as the National Bank Act.

Additionally, many banking organizations that are subject to regulation by the federal banking agencies may find the highly-detailed, static nature of the Proposed Regulations to require the application of "one size fits all" cybersecurity measures. Over the years, federally-regulated banking organizations have implemented robust cybersecurity measures under the Gramm-Leach-Bliley, Bank Protection, and Bank Service

Company Acts and their implementing regulations. These banking organizations and their federal regulators view cybersecurity as a risk-based iterative process under which regulators communicate new tailored expectations to banking organizations through the examination process and supervisory guidance (for example, the Federal Financial Institutions Examination Council published revised IT risk management guidance in November 2015 and revised information security guidance in September 2016). By contrast, the Proposed Regulations include some very specific technical requirements (e.g., multi-factor authentication and encryption). Unless DFS regularly updates its technical requirements, banking organizations may need to take additional measures in the future that are consistent with current best practices rather than the static requirements of the Proposed Regulations.

Consumer Lending. Licensed lenders, sales and premium finance companies, service contract providers, credit counselors, and mortgage bankers, brokers, loan originators, and loan servicers in New York ("consumer lenders") will be required to comply with the Proposed Regulations. While consumer lenders generally are subject to a federal obligation to secure customer information under the Federal Trade Commission's ("FTC's") Safeguards Rule, the Proposed Regulations would go significantly further in requiring the implementation of highly-specific cybersecurity measures.[4]

Consumer lenders such as mortgage brokers and loan originators frequently serve in an intermediary role, connecting customers with an array of other service providers. These consumer lenders may find it cost prohibitive to continue relationships with certain smaller service providers if they are required to conduct annual assessments of the service provider's cybersecurity practices and upgrade shared information technology systems to meet the Proposed Regulation's encryption and authentication requirements.

Further, most consumer lenders are unlikely to be able to rely on the limited exemption of Section 500.18 of the Proposed Regulations because most lenders will have more than 1,000 customers or $5 million in gross revenue on an annual basis. As with money transmitters, consumer lenders may consider using the comment period to request a more tailored application of the Proposed Regulations to non-depository entities that reflects a more risk-based approach to cybersecurity.

Money Transmitters. Money transmitters licensed by DFS will be subject to the Proposed Regulations. Money transmitter licensees will face many of the same issues as consumer lenders (described above). Money transmitters should also examine carefully how the Proposed Regulations will affect their relationships with agents in New York.

Like consumer lenders, money transmitters generally are subject to a federal obligation to secure customer information under the FTC's Safeguards Rule. As explained above, the Proposed Regulations go significantly further than the Safeguards Rule by requiring the implementation of highly specific cybersecurity measures. Money transmitters should investigate whether their current cybersecurity measures meet the specific standards in the Proposed Regulations.

The requirements of the Proposed Regulations that are related to oversight of TSPs could also apply to the relationships between money transmitters and some—but likely not all—of their agents. The extent to which a money transmitter will need to make changes to its agent relationships will depend on two factors: (1) the extent to which the agents have access to the money transmitter's information systems; and (2) whether the agents come into possession of NPI. If an agent does not have access to the money transmitter's information systems and

the agent never comes into possession of NPI, then the TSP oversight provisions will not apply.

Money transmitters would be required to implement written policies and procedures designed to ensure the security of information systems that are "accessible to" TSPs. Money transmitters should consider asking DFS to clarify what level of access to an information system makes the system "accessible to" a TSP. For example, an agent that sells a money transmitter licensee's prepaid cards generally must interface with the licensee's computer systems in order to notify the licensee that a card has been purchased and to inform the licensee how much has been loaded on the card (if it is a variable-load card). The agent will then receive confirmation from the licensee's system that the card has been activated. A reasonable argument could be made that exchanging basic information about a transaction with an agent through an information system does not make the information system "accessible to" the agent, but this could be clearer.

Agents of money transmitters also do not always receive NPI in connection with money transmission transactions. For example, the customer does not provide, and the agent does not otherwise receive, any NPI in connection with the sales of most prepaid cards. (Most prepaid card products sold at retail locations are designed not to trigger customer identification requirements under anti-money laundering laws, so these cards are sold "anonymously.") However, agents might receive NPI from either the customer or the money transmitter in a money transfer transaction. To effect a money transfer, the sending agent must at least receive information from the customer about the recipient of the transfer. The disbursing agent must receive information about the transaction from the money transmitter. Because of how broadly NPI is defined (it includes any information that an individual provides in connection with the seeking or obtaining of a financial product or service, regardless of whether the information is sensitive or confidential), it appears that agents in these remittance transactions would not be able to avoid receiving NPI. If so, this would trigger the TSP oversight provisions.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

David L. Beam
+1 202 263 3375
dbeam@mayerbrown.com

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

Lawrence R. Hamilton
+1 312 701 7055
lhamilton@mayerbrown.com

Brad L. Peterson
+1 312 701 8568
bpeterson@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

David A. Tallman
+1 713 238 2696
dtallman@mayerbrown.com

James R. Woods
+1 212 506 2390
jrwoods@mayerbrown.com

Matthew G. Gabin
+1 212 506 2321
mgabin@mayerbrown.com

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

Endnotes

[1] Letter from Anthony J. Albanese (Nov. 9, 2015).

[2] DFS, *Cybersecurity Requirements for Financial Services Companies* (proposed Sept. 13, 2016).

[3] DFS also supervises certain government-sponsored entities, such as the New York Business Development Corporation and State of New York Mortgage Agency. The Proposed Regulations do not specify if these quasi-governmental entities would be subject to the cybersecurity standards.

[4] Other than the requirements outlined in the consent order with Dwolla, Inc., the Consumer Financial Protection Bureau has not addressed cybersecurity practices.