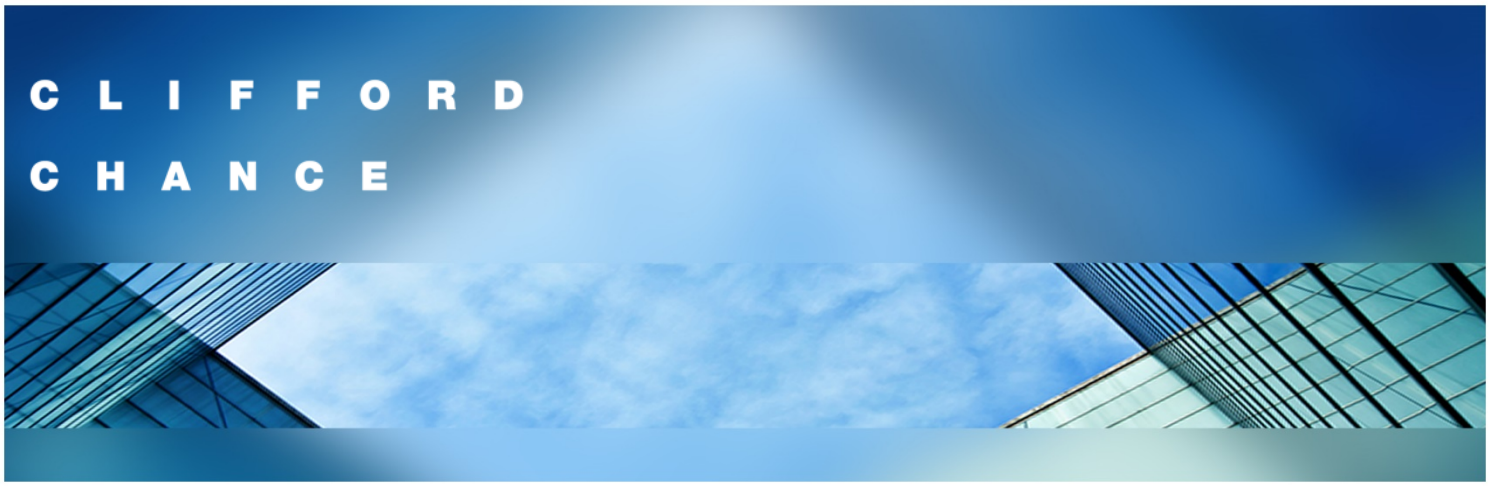

THIRD TRANSITIONAL PERIOD UNDER NY DFS CYBERSECURITY RULES ENDS SEPTEMBER 4, 2018

As New York State Department of Financial Services ("DFS") Superintendent Maria T. Vullo reminded regulated entities last week, the third transitional period of DFS's Cybersecurity Rules, 23 NYCRR Part 500, ends on September 4, 2018, meaning that banks, insurance companies, and other financial services providers covered by the Cybersecurity Rules will be required to comply with rules regarding annual reporting to the board, audit trails, application security, limitations on data retention, encryption, and certain training and monitoring requirements. Although no reporting or certification requirement accompanies the September 4, 2018 deadline, covered entities would be well advised to comply with these requirements so that compliance can be demonstrated if DFS examiners come calling[1] or when the compliance certifications are next due in February 2019.[2]

KEY REQUIREMENTS UNDER THE CYBERSECURITY RULES THAT ARE NOW IN EFFECT

As we have previously summarized, the Cybersecurity Rules are an unprecedented action by a state government agency and contain strict requirements for DFS-licensed entities ("Covered Entities") to establish enhanced cybersecurity programs, adopt written cybersecurity policies and procedures, and report cyber-events to DFS. By now, Covered Entities should already have in place a Cybersecurity Program and policies and procedures; a Chief Information Security Officer ("CISO"); limitations on access privileges to non-public information; and an incident response plan. Certain other requirements of the Rules will come into effect on September 4, 2018 and full compliance will be expected and required in March of 2019.

The requirements that must be put into place by September 4, 2018 include:

---

1 DFS has announced that it will be incorporating cybersecurity in all of its examinations of financial services companies.

2 See 23 NYCRR 500.17(b).

Mandatory Annual Reporting (500.04(b))

The Cybersecurity Rules require the CISO to report in writing at least once a year to the Covered Entity's board of directors (or equivalent) on the entity's cybersecurity program and material cybersecurity risks. This requirement ensures that the leadership of a Covered Entity is fully aware of the cybersecurity health of the company and that it considers cybersecurity risks in governance decisions. Technically, this requirement came into effect at the end of the second transitional period, which ended on March 1, 2018, so Superintendent Vullo's focus on annual reporting in her reminder may suggest the importance DFS assigns to it. Thus, Covered Entities that have not yet had their CISO produce a written report should at least have a plan in place to meet the mandatory annual reporting requirement.

Audit Trail (500.06)

The Cybersecurity Rules' audit trail requirement is aimed at ensuring that Covered Entities can continue to operate normally in the event of a breach. Breaches are mostly associated with data theft, but data destruction often also accompanies a breach, either as collateral damage used to cover up an attackers' tracks or on occasion as the primary purpose of the breach. Having records that allow the Covered Entity to continue to operate normally (such as, for example, having a system of continuous backups) will help mitigate the destruction caused by a breach. Covered Entities are also required to have audit trails designed to detect and respond to Cybersecurity Events, meaning their systems should have some way of detecting and logging user access to identify unauthorized entry.

Application Security (500.08)

Under the Cybersecurity Rules, Covered Entities must ensure that the programs and applications they use are secure. This means that they must have written procedures, guidelines, and standards in place for internally-developed applications to minimize the possibility of adding security vulnerabilities to the company's systems. They must also have procedures for evaluating and testing externally-developed applications. The CISO or her designee is in charge of these procedures and must review, assess, and update these rules periodically, beginning in September.

Limitations on Data Retention (500.13)

Covered Entities are no longer allowed to retain information indefinitely without a legitimate business purpose under the Cybersecurity Rules. Instead, Covered Entities are required to have in place policies and procedures for the periodic secure disposal of Nonpublic Information that is no longer needed for business operations or another legitimate business purpose. The exceptions to this rule are (1) if the information is required to be retained by law or regulation; or (2) targeted disposal is not reasonably feasible due to the manner in which the information is maintained. Nonpublic information is information that is not publicly available and includes: (1) business information that would cause a material adverse impact on the business if lost, stolen, or damaged; (2) personal information that can be linked to a specific individual, including social security number, drivers' license or other identification card numbers, financial account numbers, access to an individual's financial account, or biometric records; or (3) health information

relating to the physical, mental, or behavioral health condition of an individual or her family.

Training and Monitoring (500.14(a))

The Cybersecurity Rules requires Covered Entities to implement risk-based policies, procedures, and controls designed to monitor the activity of authorized users to help detect unauthorized access or use of (or tampering with) nonpublic information (as described above). One interesting note on this requirement is that the wording of the Rule explicitly specifies that the provision is aimed at detecting intruder access, not overseeing authorized users' activity. Covered Entities may nonetheless want to consider whether certain controls should also be put in place to ensure that authorized users' activity does not also create the risk of a cybersecurity breach.

Encryption (500.15)

Covered Entities are required to implement systems that can encrypt nonpublic information—both "in transit" and "at rest"—as part of their cybersecurity compliance to protect that data from unauthorized access, disclosure, or destruction. Encryption may pose challenges especially for data "at rest" in legacy computer systems stored internally. There are exceptions to this policy for when encryption is infeasible, but to take advantage of this exception the Covered Entity must establish alternative data protection mechanisms such as requiring recipients to use their own controls, and the feasibility of encryption must be evaluated at least once a year. As a result, Covered Entities should seek to implement encryption solutions, if at all possible.

CONCLUSION & IMPLICATIONS

The Superintendent's recent reminder is the latest of many signals that cybersecurity is and will continue to be a key focus at DFS. Compliance with the Cybersecurity Rules has already been incorporated in DFS's examinations and will likely be a priority in those examinations moving forward. Covered Entities should in turn make compliance with the Rules a priority as well.

Covered Entities may also want to keep an eye on what other states are doing in the cybersecurity and data privacy space. In July we wrote about California's newly enacted California Consumer Privacy Act of 2018, a sweeping regulation modelled after Europe's General Data Protection Regulation aimed at protecting consumer personal data. Other states may follow California's example, which may in turn affect New York State's approach to its own Rules.

Covered Entities will also want to look ahead to the Rules' final transitional phase, which requires them to ensure that their third party service providers also comply with the Cybersecurity Rules' requirements.

AUTHORS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

KEY CYBERSECURITY CONTACTS

Alexander Anichkin
Partner, Moscow

T +7 495 258 5089
E alexander.anichkin
@cliffordchance.com

Carlo Felice Giampaolino
Partner, Milan

T +39 064229 1356
E carlofelice.giampaolini
@cliffordchance.com

Megan Gordon
Partner, Washington, DC

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Tim Grave
Partner, Sydney

T +61 2 8922 8028
E tim.grave
@cliffordchance.com

Luke Grubb
Partner, Singapore

T +65 6506 2780
E luke.grubb
@cliffordchance.com

Ling Ho
Partner, Hong Kong

T +852 2826 3479
E ling.ho
@cliffordchance.com

Alice Kane
Counsel, New York

T +1 212 878 8110
E alice.kane
@cliffordchance.com

Jonathan Kewley
Partner, London

T +44 20 7006 3629
E jonathan.kewley
@cliffordchance.com

Alvin Khodabaks
Partner, Amsterdam

T +31 20 711 9374
E alvin.khodabaks
@cliffordchance.com

Anita Lam
Consultant, Hong Kong

T +852 2825 8952
E anita.lam
@cliffordchance.com

Markus Muhs
Partner, Munich

T +49 89 21632 8530
E markus.muhs
@cliffordchance.com

Lena Ng
Partner, Singapore

T +65 6410 2215
E lena.ng
@cliffordchance.com

Masayuki Okamoto
Partner, Tokyo

T +81 3 6632 6665
E masayuki.okamoto
@cliffordchance.com

Daniel Royle
Partner, Abu Dhabi

T +966 11481 9756
E daniel.royle
@cliffordchance.com

Dessislava Savova
Partner, Paris

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com

CLIFFORD
CHANCE

Daniel Silver
Partner, New York

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Natsuko Sugihara
Partner, Tokyo

T +81 3 6632 6681
E natsuko.sugihara
@cliffordchance.com

Luke Tolaini
Partner, London

T +44 20 7006 4666
E luke.tolaini
@cliffordchance.com

Arun Visweswaran
Senior Associate, Dubai

T +971 4503 2748
E arun.visweswaran
@cliffordchance.com

Donna Wacker
Partner, Hong Kong

T +852 2826 3478
E donna.wacker
@cliffordchance.com