LEWIS BRISBOIS®

What do the New York Cybersecurity Regulations Teach Counsel Representing Insurance Companies & their Insureds About "Reasonable Efforts" to Protect Confidential Information?

Gordon J. Calhoun

Partner, San Francisco
Gordon.Calhoun@lewisbrisbois.com
213.680.5141

Gordon Calhoun serves as the chair of the Electronic Discovery, Information Management & Compliance Practice and manages the insurance regulatory and reinsurance division of the firm's Insurance Coverage and Bad Faith Practices.

Barry G. Kaiman

Partner, Los Angeles
Barry.Kaiman@lewisbrisbois.com
213.680.5053

Barry Kaiman serves as the chair of the firm's Government Relations Practice. He has over 40 years of experience in the areas of professional liability, insurance coverage and bad faith defense, among other practices.

WHAT DO THE NEW YORK CYBERSECURITY REGULATIONS TEACH COUNSEL REPRESENTING INSURANCE COMPANIES AND THEIR INSUREDS ABOUT "REASONABLE EFFORTS" TO PROTECT CONFIDENTIAL INFORMATION?

I. INTRODUCTION: ETHICAL RULES IMPOSE A FIDUCIARY OBLIGATION TO PREVENT UNAUTHORIZED DISCLOSURES OF CONFIDENTIAL INFORMATION.

While both the ethical duty of confidentiality and the evidentiary principle of the attorney-client privilege relate to duties owed with respect to information held by a lawyer, they are distinct concepts with separate standards. Communications protected by the attorney-client privilege are a subset of information a lawyer must keep confidential. The attorney-client privilege protects only confidential communications between attorney and client that are made to facilitate the rendition of legal services. The obligation to protect non-public information received from or about clients is much broader. While the duty of confidentiality allows disclosure in certain situations, such as when disclosure is necessary to abide by a court order or under the ethical rules in many jurisdictions to prevent a crime or harm to others, the privilege, if it applies to a communication, is exempt from court compulsion in some jurisdictions and subject to limited *in camera* examination in others.

The focus of this discussion will be on all data types an attorney must keep confidential. Because of the duty of confidentiality, established by American Bar Association ("ABA") Model Rule 1.6[1] and California's Rules of Professional Conduct ("CRPC")[2], a lawyer has an obligation not to disclose information acquired in the course of representing a client, unless authorized by the client, the information is publicly available or the information falls within established exceptions to the ABA and CRPC rules[3].

---

1 ABA Model Rule 1.6(a) provides, "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)."

2 CRPC Rule 3-100(A) provides, "(A) A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client, or as provided in paragraph (B) of this rule."

3 For example, ABA Model Rule 1.6(b) enumerates s number of exceptions:

"(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

"(1) to prevent reasonably certain death or substantial bodily harm;

"(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

"(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

"(4) to secure legal advice about the lawyer's compliance with these Rules;

"(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

"(6) to comply with other law or a court order; or

"(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition

ABA Model Rule 1.6(c) imposes a duty to preserve the confidentiality of this information, but does little to define what counsel must do to meet this duty[4]. Comment 16 to Model Rule 1.6 imposes on counsel a duty to understand how to use appropriate technologies to protect confidential client information. It provides, "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." When combined with Rule 1.1 about competence and the commentary on it, there remains little doubt that counsel are obligated to be aware of current technologies for safeguarding information and to regularly audit those safeguards to make sure they are adequate to the task.

II. FEDERAL AND STATE STATUTES AND REGULATIONS HAVE BEGUN TO IMPOSE STANDARDS FOR THE PROTECTION OF SPECIFIC TYPES OF INFORMATION, WHICH BIND LAWYERS RECEIVING IT.

Some guidelines exist for specialized types of confidential information. At the federal level, an attorney who receives protected health information ("PHI") from a Covered Entity under the Health Insurance Portability & Accountability Act (HIPAA) will generally be a "business associate" and be required to comply with the HIPAA security requirements. The 2009 HIGHTECH Act enhanced HIPAA security requirements, extended them directly to business associates, and added a new breach notification requirement. The regulations do not apply to PHI obtained from other sources, however. There are protections afforded to PHI by most states' laws which are not limited to data received from Covered Entities, which must be observed. For other types of information, such as personally identifiable financial information ("PII"), the FTC's Safeguards Rule under the Gramm-Leach-Bliley Act provides a helpful framework lawyers can use to satisfy their obligations to safeguard client data. The requirements in the rule, *Standards for Safeguarding Customer Information*, 16 C.F.R., Part 314, are general and cover less than two pages in the Federal Register. They provide a short yet comprehensive list of the components of a complete security program.

---

or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client."

CRPC 3-100(B)-(E), which define when a lawyer may disclose confidential information, provide:

"(B) A member may, but is not required to, reveal confidential information relating to the representation of a client to the extent that the member reasonably believes the disclosure is necessary to prevent a criminal act that the member reasonably believes is likely to result in death of, or substantial bodily harm to, an individual.

"(C) Before revealing confidential information to prevent a criminal act as provided in paragraph (B), a member shall, if reasonable under the circumstances:

"(1) make a good faith effort to persuade the client: (i) not to commit or to continue the criminal act or (ii) to pursue a course of conduct that will prevent the threatened death or substantial bodily harm; or do both (i) and (ii); and

"(2) inform the client, at an appropriate time, of the member's ability or decision to reveal information as provided in paragraph (B).

"(D) In revealing confidential information as provided in paragraph (B), the member's disclosure must be no more than is necessary to prevent the criminal act, given the information known to the member at the time of the disclosure.

"(E) A member who does not reveal information permitted by paragraph (B) does not violate this rule."

4 "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

For larger law firms, standards published by the International Organization for Standardization (ISO), at www.iso.org, provide a useful framework. They include ISO/IEC 17799:2005, *Information Technology—Code of Practice for Information Security Management* and ISO/IEC 27001:2005, *Information Technology—Security Techniques—Information Security Management System—Requirements*.

III. NEW YORK'S DEPARTMENT OF FINANCIAL SERVICES PROMULGATED "CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES," WHICH APPLY TO "COVERED ENTITIES," INCLUDING INSURANCE COMPANIES DOING BUSINESS IN NEW YORK, AND TO LAWYERS WHO ARE DEEMED "THIRD-PARTY SERVICE PROVIDERS" TO INSURERS.

A. Introduction.

What is required of lawyers representing insurance companies and financial institutions subject to regulation in New York state just became a lot more precise. Compliance will be measured by metrics much more stringent than "reasonable efforts" as a result of recently adopted cybersecurity regulations. They put more meat on the bones of an attorney's duty to protect certain types of confidential information. We can reasonably anticipate the standards developed for confidential information received from insurance companies and financial institutions will expand to all types of confidential information received by attorneys and that they will be expected to adopt the policies, procedures, protocols and technologies needed to comply with the New York Regulations.

New York has positioned itself as a leader on data security and privacy issues affecting the insurance and financial industries by implementing one of the most detailed, stringent and comprehensive data security regulations to date. Unlike HIPAA, Gramm-Leach-Bliley or even state privacy protections, the Regulations are omnibus in scope. They apply to all confidential information relating to a customer regardless of its type or content possessed by an insurer or financial institution. These "Cybersecurity Requirements for Financial Services Companies" regulations can be found at 23 NYCRR §§ 500, *et seq.,* and as Appendix I to this paper. They became effective on March 1, 2017. These Regulations represent a new approach targeting the financial and insurance industries, and as discussed below, those persons and entities like attorneys, law firms, consultants, expert witnesses, court reporters, eDiscovery technology providers, etc. offering services to Covered Entities and their insureds. The Regulations call these parties subject to the jurisdiction of the New York Department of Financial Services ("DFS") Third-Party Service Providers.

The reason for the Regulations is obvious. New York is a prime target for those looking to steal financial information. New York City is one of the world's most significant financial communities, and a massive volume of financial data is stored and processed there. In the age of big data, and in the face of constantly escalating threats to the security of private information, insurance companies and financial institutions must do their part to protect their consumers' nonpublic information. And this new Regulation extends that obligation to third parties who also touch consumer data. If you are doing business with any Covered Entity you are subject to this regulation, and must adhere to specific requirements set out the rule—regardless of where you are performing that service or what your underlying function may be.

To bolster the security of this information, DFS created and implemented a new set of regulations designed to force certain regulated businesses to employ policies, procedures and technologies needed to protect confidential consumer and corporate information, financial and otherwise. While not necessarily controversial, the requirements of these Regulations could be confusing and potentially onerous to those unfamiliar with cybersecurity best practices.

B. The Regulations Apply to "Covered Entities," Including All Insurers Doing Business In New York.

The Cybersecurity Regulation applies to all "Covered Entities," which includes all individuals and non-governmental entities (*i.e.*, corporations, partnerships, associations, etc.) "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." (23 NYCRR § 500.01(c).) For all practical purposes, any business in the insurance and financial services industries that is not a government agency transacting in New York is covered by these Regulations. They cast a very broad net. Many organizations, which are not traditional banks or insurance companies, are still required to obtain certificates, permits or other authorizations under the applicable laws and will be required to comply with the Regulations.

C. The Regulations Also Apply to "Third-Party Service Providers," Including Attorneys.

The new DFS Regulations reflect the reality those serving financial institutions, particularly banks, have operated under for years: Because many financial services companies have long expressed their fear of third party service providers experiencing a cybersecurity breach, they have imposed stringent security assessment requirements on their Third-Party Service Providers, including lawyers. What is comparatively new is extending these strictures to law firms, which provide traditional insurance defense services to insureds involved in litigation.

New York's Regulations expand those strict requirements to other business partners not typically viewed as "service providers," such as law firms, many of which historically were not subjected to rigorous security audits from clients and relied on evidentiary privileges as the principle bulwark against inappropriate access to client confidences.

The Regulations reach lawyers and others providing services to Covered Entities because they are deemed to be Third-Party Service Providers. They are defined as "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." (23 NYCRR § 500.01(n).) Following a model similar to that established by cybersecurity and data privacy regulations created for the healthcare industry by HIPAA and the HITECH Act, regulators will exercise direct and indirect control over both Covered Entities and Third-Party Service Providers in much the same way the Office of Civil Rights regulates healthcare providers, called Covered Entities, and their service providers called Business Associates.

D. Some Regulations Are Already in Effect and Others Will Phase in Until March 2019.

Because of the sweeping scope of the Regulations, there are transition periods (ranging from 180 days to two years) for compliance with certain requirements of the Regulations. These important dates are set forth below:

- **March 1, 2017** - 23 NYCRR Part 500 becomes effective.
- **August 28, 2017** - 180 day transitional period ends. Covered Entities are required to be in compliance with requirements of 23 NYCRR Part 500 unless otherwise specified.
- **February 15, 2018** - Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date.
- **March 1, 2018** - One year transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500.
- **September 3, 2018** - Eighteen month transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of 23 NYCRR Part 500.
- **March 1, 2019** - Two year transitional period ends. Covered Entities are required to be in compliance with the requirements of 23 NYCRR 500.11.

The reason why these dates are important to lawyers and law firms providing services to insureds covered by insurers regulated by DFS is the Regulations also impose requirements on "Third-Party Service Providers, which includes any lawyer or law firm that "maintains, processes or otherwise is permitted access to" nonpublic information through its provision of services to" an insurer subject to regulation by DFS. (23 NYCRR § 500.01(n).) So any person or organization, including lawyers and law firms, doing business with a New York insurance or financial institution and accessing its sensitive information must adhere to the cybersecurity provisions set out in the new Regulations.

E. Compliance Is Expected to be Complete as Soon as Each Critical Date Is Reached.

Over the past two decades, as data security standards, like HIPAA and HITECH, phased in, enforcement was often lax for many years as regulators and those subject to the regulations struggled to understand how the standards ought to be applied and what was required for compliance. That learning period is effectively over in the healthcare space. DFS is sending a message that it will not be as restrained as the Office of Civil Rights, the enforcement agency charged with implementing the HIPAA Regulations, about working with those subject to regulation.

Among the Frequently Asked Questions ("FAQs") on the DFS website is one addressing whether literal compliance with the upcoming February 15, 2018 deadline is expected. In response to the FAQ, "Is a Covered Entity required to certify compliance with all the requirements of 23 NYCRR 500 on February 15, 2018?**,"** DFS responds:

> "Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) by February 15, 2018. This initial certification applies to and includes all requirements of 23 NYCRR Part 500 for which the applicable transitional period under 23 NYCRR 500.22 has terminated prior to February 15, 2018. Accordingly, Covered Entities will not be required to submit certification of compliance with the requirements of 23 NYCRR 500.04(b), 500.05, 500.06, 500.08, 500.09, 500.12, 500.13, 500.14 and 500.15 until February 15, 2019, and certification of compliance with 23 NYCRR 500.11 until February 15, 2020."

New York regulators signaled they intend to be aggressive when enforcing the regulations. There is no reason not to take them at their word. This means Covered Entities, like insurance companies and financial institutions, must comply as quickly as possible, which creates issues for those who provide professional services to these industries. For example, in one of the many FAQs on the DFS website asks, "May a Covered Entity submit a certification under 23 NYCRR 500.17(b) if it is not yet in compliance with all applicable requirements of Part 500?" The response exhibits little flexibility. The only exception to full compliance are carve outs provided for by the transitional provisions. DFS states**:**

> "The Department expects ***full*** compliance with this regulation. A Covered Entity may not submit a certification under 23 NYCRR 500.17(b) unless the Covered Entity is in compliance with all applicable requirements of Part 500 at the time of certification. To the extent a particular requirement of Part 500 is subject to an ongoing transitional period under 23 NYCRR 500.22 at the time of certification, that requirement would not be consider applicable for purposes of a certification under 23 NYCRR 500.17(b). (Added emphasis.)

The insurance companies routinely engage the services of consultants, including eDiscovery technology providers, consultants, expert witnesses, photocopying and imaging services, court reporters, etc., who receive nonpublic information about insureds. They are often engaged by lawyers and both the lawyers and their insurance company clients will be responsible for how these second or third level Third-Party Service Providers handle that confidential information. Bottom line—any organization dealing with a Covered Entity's nonpublic information must step up and comply with the Regulations' requirements around cybersecurity.

IV. DUTIES IMPOSED ON COVERED ENTITIES AND ON THIRD-PARTY SERVICE PROVIDERS.

A. Introduction.

The Cybersecurity Regulations impose new requirements on Covered Entities designed to implement policies, procedures and technical protections to prevent unauthorized access to confidential data. These

Regulations are important to lawyers serving insurance companies and other financial institutions operating in New York because the Covered Entities must ensure those providing services to them, *i.e.*,Third-Party Service Providers, are also compliant with the Regulation. Lawyers providing professional services to Covered Entities subject to the Cybersecurity Regulation must comply with its terms. Otherwise, they will subject their clients, the insurers, to liability under the Regulations.

Every Covered Entity must develop a Third-Party Service Provider Security Policy. Third-Party Service Provider Security Policy – The Cybersecurity Regulation specifically identifies the risks posed by the use of third parties in handling financial or customer data. Whenever data is moved between systems, risks and vulnerabilities are often exposed and can be exploited. Entities are expected to incorporate third parties into their Risk Assessment and perform the necessary due diligence to ensure that Third-Party Service Providers, including lawyers, provide sufficient security to the data they receive from Covered Entities. A regulated entity must implement written policies and procedures, based on the entity's risk assessment, designed to ensure the security of information systems and data accessible to or held by the entity's Third-Party Service Providers.

The policies and procedures, and related guidelines Covered Entities must implement are required to address, to the extent applicable, risk identification and assessment of Third-Party Service Providers, minimum required cybersecurity practices to be followed by Third-Party Service Providers, due diligence processes for assessing Third-Party Service Providers' cybersecurity practices and periodic reassessments of Third-Party Service Providers.

Third-Party Service Providers will have to meet situationally appropriate data security standards in order to continue working for Covered Entities. One of the FAQs on the DFS website asks, "Are all Third-Party Service Providers required to implement Multi-Factor Authentication and encryption when dealing with a Covered Entity?" DFS responds by stating:

> "23 NYCRR 500.11, among other things, generally requires a Covered Entity to develop and implement written policies and procedures designed to ensure the security of the Covered Entity's Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers. 23 NYCRR 500.11(b) requires a Covered Entity to include in those policies and procedures guidelines, as applicable, addressing certain enumerated issues. Accordingly, 23 NYCRR 500.11(b) requires Covered Entities to make a risk assessment regarding the appropriate controls for Third-Party Service Providers based on the individual facts and circumstances presented and does not create a one-size-fits-all solution."

To meet the obligations imposed by the Regulations, a Covered Entity must perform a risk assessment of its Third-Party Service Providers and conduct due diligence to evaluate the adequacy and the practices of such third parties. Covered Entities must also continue to periodically assess the third parties as part of their ongoing assessment and include all contractual provisions, such as multi-factor authentication, encryption, notification of cybersecurity events, and representations and warranties related to cybersecurity policies in their agreements.

DFS acknowledges that these obligations impose a substantial burden to Covered Entities and will require Covered Entities to update internal form agreements and conduct extensive, intrusive audits of their Third-Party Service Providers. As a result, the DFS is allowing Covered Entities, including exempt entities, two years to implement this Regulation (to March 1, 2019).

B. What DFS Requires of Covered Entities and the Third-Party Service Providers Providing Professional Services to Them.

Among the requirements with which Covered Entities, and by extension their lawyers, must comply are the following:

- **Develop a Cybersecurity Program** – Covered entities must create, document and implement an internal cybersecurity policy. This policy must be based on a risk assessment (described below), and implements "defensive infrastructure and ... policies and procedures" to protect the financial data the entity possesses. (23 NYCRR 500.02.)

- **Implement a Cybersecurity Policy** – The Cybersecurity Program described above must be documented in the form of a comprehensive Cybersecurity Policy. This policy must be approved by company leadership 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
  - System operations and availability measures
  - System and network security
  - Systems and network monitoring
  - Systems and application development and quality assurance
  - Physical records security
  - Vendor and Third-Party Service Provider management
  - Risk assessment
  - Incident response (23 NYCRR 500.03)

- **Appoint a Chief Information Security Officer** – Each Covered Entity must appoint a Chief Information Security Officer ("CISO"), whose role it is to lead the company's Cybersecurity Program and oversee the creation and implementation of the Cybersecurity Policy. (23 NYCRR 500.04)

- **Train Personnel about Cybersecurity/Keep Their Knowledge Current:** A Covered Entity must: (1) engage qualified cybersecurity personnel, in addition to its CISO, sufficient to manage the entity's cybersecurity risks and perform or oversee performance of the entity's cybersecurity program; (2) provide its cybersecurity personnel with sufficient cybersecurity updates and training; and (3) verify that its cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. The required cybersecurity personnel may be sourced from an affiliate of the entity or an independent Third-Party Service Provider.

- **Adopt and Train Staff about Duties Under an Incident Response Plan** – All Covered Entities must create and implement an incident response plan ("IRP"). An IRP is a documented, practices and tested policy that outlines the steps that are taken by all relevant employees in the event of a suspected or actual data breach.

- **Conduct Annual Penetration Testing and Bi-Annual Vulnerability Assessments** - The entity's program must include annual penetration testing of vital systems and bi-annual system scans to assess the system and network requirements for known vulnerabilities. (23 NYCRR 500.05)

- **Conduct Periodic Risk Assessment Audits** – The Cybersecurity Regulation includes a requirement that each covered entity perform a risk assessment based on written policies and procedures created and documented within the Cybersecurity Policy. This risk assessment is performed on the Covered Entity's computer and network systems and forms the backbone of the Cybersecurity Program. The risk assessment is designed to highlight the major risks to the Covered Entity's financial data, customer or client data, and other sensitive data and assist the entity in understanding how data flows through its systems and where it is most vulnerable. The Risk Assessment should be periodically revisited and updated as necessary. (23 NYCRR 500.09

- **Implement Multi-factor Authentication or Its Equivalent** – Now, under the Cybersecurity Regulation, all Covered Entities must utilize multi-factor authentication technologies for all remote-access services, unless the Covered Entity's CISO has approved the use of reasonably equivalent remote access controls. (23 NYCRR 500.12)

- **Encrypt All Sensitive Data While in Motion or at Rest** – The Cybersecurity Regulation also requires that nonpublic information is encrypted while in motion and while at rest unless this encryption is infeasible. If such a determination is made, it must be documented and revisited by the CISO at least annually. The kind and strength of the encryption is not provided by the Cybersecurity Regulation. (23 NYCRR 500.15.)

- **Create Audit Trails to Assist with Detection and Response to Intrusions** – A Covered Entity must maintain systems that, to the extent applicable based on its risk assessment, are designed to reconstruct material transactions sufficient to support the entity's normal operations and obligations and include audit trails designed to detect and respond to cybersecurity events that are likely to materially harm the entity's normal operations. The records created by those systems must be maintained for minimum retention periods. (23 NYCRR 500.06)

- **Limit Access Privileges to Those Who Need to Know - -** Limited user access privileges to the entity's information systems that contain sensitive data, and periodic review of those access privileges. (23 NYCRR 500.07.)

- **Develop Application Security and Update Regularly - -** Written procedures, guidelines and standards for the security of software applications (both internally and externally developed) used by the Covered Entity in its technology environment. The procedures, guidelines and standards must be periodically reviewed, assessed and updated. (23 NYCRR 500.08.)

- **Limit Data Retention to that Which Serves Business Purposes or Is Required for Compliance --** Secure, periodic disposal of data that is no longer necessary for the Covered Entity's business operations or legitimate business purposes, except where a legal retention requirement applies or targeted disposal is not feasible. (23 NYCRR 500.13.)

- **Monitoring of Systems and Training Personnel**: Risk-based monitoring of authorized users to detect unauthorized access to or use of data, and regular cybersecurity awareness training for all personnel. (23 NYCRR 500.05.)

DFS defines wat constitutes "continuous monitoring" for purposes of 23 NYCRR 500.05. It explains effective continuous monitoring could be attained through a variety of technical and procedural tools, controls and systems. There is no specific technology that is required to be used in order to have an effective continuous monitoring program. Effective continuous monitoring generally has the ability to continuously, on an ongoing basis, detect changes or activities within a Covered Entity's Information Systems that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity. In contrast, non-continuous monitoring of Information Systems, such as through periodic manual review of logs and firewall configurations, would not be considered to constitute "effective continuous monitoring" for purposes of 23 NYCRR 500.05.

C. Responding to a Data Security Incident Requires Notification within 72 Hours if a Breach Occurs and May Require Reporting Even in the Absence of a Breach if They Raise a Serious Concern.

The Department recognizes that Covered Entities' focus should be on preventing cybersecurity attacks and improving systems to protect the institution and its customers. The Department's notice requirement is intended to facilitate information sharing about serious events that threaten an institution's integrity and that may be relevant to the Department's overall supervision of the financial services industries. The Department trusts that Covered Entities will exercise appropriate judgment as to which unsuccessful attacks must be reported and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment. The question of "**When is a Covered Entity required to report a Cybersecurity Event under 23 NYCRR 500.17(a)?"** is answered on the DFS website as follows:

> "23 NYCRR 500.17(a) requires Covered Entities to notify the superintendent of certain Cybersecurity Events as promptly as possible but in no event later than 72 hours from a

determination that a reportable Cybersecurity Event has occurred. A Cybersecurity Event is reportable if it falls into at least one of the following categories:

- the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

- the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

"An attack on a Covered Entity may constitute a reportable Cybersecurity Event even if the attack is not successful."

The Department recognizes that Covered Entities and Third-Party Service Providers are regularly subject to many attempts to gain unauthorized access to, disrupt or misuse Information Systems and the information stored on them, and that many of these attempts are thwarted by the Covered Entities' cybersecurity programs. The Department anticipates that most unsuccessful attacks will *not* be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern. For example, notice to the Department under 23 NYCRR Section 500.17(a)(2) would generally *not* be required if, consistent with its Risk Assessment, a Covered Entity makes a good faith judgment that the unsuccessful attack was of a routine nature.

The Department explains when an unsuccessful attack which raises "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" as specified by the reporting requirements of 23 NYCRR Section 500.17(a)(2). The Department believes that analysis of unsuccessful threats is critically important to the ongoing development and improvement of cybersecurity programs, and Covered Entities are encouraged to continually develop their threat assessment programs. Notice of the especially serious unsuccessful attacks may be useful to the Department in carrying out its broader supervisory responsibilities, and the knowledge shared through such notice can be used to timely improve cybersecurity generally across the industries regulated by the Department. Accordingly, Covered Entities are requested to notify the Department of those unsuccessful attacks that appear particularly significant based on the Covered Entity's understanding of the risks it faces. For example, in making a judgment as to whether a particular unsuccessful attack should be reported, a Covered Entity might consider whether handling the attack required measures or resources well beyond those ordinarily used by the Covered Entity, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps.

Recognizing that not all companies are built alike, the regulations permit the Covered Entity to use an affiliate or "qualified" third-party service provider to assist in complying with the regulation. This alleviates the burden on smaller organizations that may not have the infrastructure or resources to implement all requirements with in-house personnel. This model may also be employed by those providing professional services to a Covered Entity.

V. CONCLUSION.

At least for lawyers providing services to insurance companies subject to regulation by DFS and probably for all lawyers, the answer to what constitutes "reasonable efforts" to protect confidential client information has become a lot more precise. The Regulations provide metrics by which the conduct of counsel may be measured. Law suits have already been filed alleging law firms have failed to protect adequately confidential information. A defense based on that absence of a breach is likely to become less compelling as regulatory agencies establish a floor for the security of confidential client information, at least for those attorneys representing companies in the insurance and financial industries.

Once that floor is established, it is likely to apply to all attorneys. There does not appear to be a defensible way to argue confidential information about a client who is an insured is subject to a higher level of protection than a similarly situated client who is not an insured. Under the ethical rules, it is the confidential information about a client that is entitled to protection. The client's status, whether an insured or not, does not enter into the applicable standard.

APPENDIX I

NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means 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.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following

data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records.

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) *Person* means any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* 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.

Section 500.02 Cybersecurity Program.

(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

(a) Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(1) information security;

(2) data governance and classification;

(3) asset inventory and device management;

(4) access controls and identity management;

(5) business continuity and disaster recovery planning and resources;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) customer data privacy;

(12) vendor and Third Party Service Provider management;

(13) risk assessment; and

(14) incident response.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and

(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's

cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;

(2) the Covered Entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the Covered Entity;

(4) overall effectiveness of the Covered Entity's cybersecurity program; and

(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

(a) The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity'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, Covered Entities shall conduct:

(1) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(2) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) 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 of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity'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 Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.09 Risk Assessment.

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise 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.

Section 500.14 Training and Monitoring.

(a) As part of its cybersecurity program, each Covered Entity shall:

(1) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(2) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity 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 Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

(a) Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B.

(e) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement.

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.21 Effective Date.

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

Section 500.22 Transitional Periods.

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

FIRM OVERVIEW

Established in 1979, Lewis Brisbois Bisgaard & Smith LLP is a national, full-service law firm with more than 1,100 attorneys and 42 offices in 26 states.

Lewis Brisbois offers legal practice in more than 40 specialties, and a multitude of sub-specialties. Our attorneys have broad knowledge, experience, and sensitivity to our clients' unique needs. Through interaction among our practice groups, Lewis Brisbois provides a wide range of legal services to each client with a continuity of representation across multiple disciplines. We have built longstanding relationships with corporate and institutional clients based on our ability to provide comprehensive service on a national scale.

At Lewis Brisbois, diversity is an integral part of our firm culture and our daily life. We accomplish diversity not by committee or initiative, but through the honest and consistent practice of hiring the best people for the job and rewarding excellence. The success of these policies is reflected in the fact that Lewis Brisbois has repeatedly received national recognition for its commitment to embracing diversity. Lewis Brisbois is committed to hiring and retaining a diverse group of talented lawyers and staff, and demonstrates that commitment through non-discriminatory hiring, retention and promotion policies. The diversity of Lewis Brisbois' client base is matched by the diversity of our attorneys.

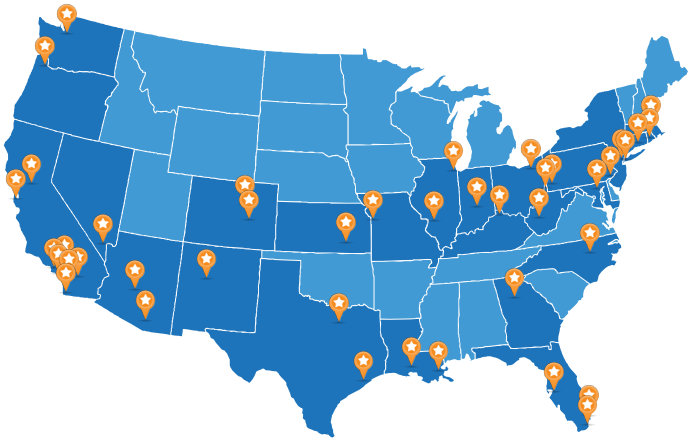
With offices from Los Angeles to New York and Seattle to Miami, our attorneys reflect the communities in which they live. Lewis Brisbois' culture has fostered a diverse group of professionals committed to promoting the best interests of our clients, our communities and the legal profession. We support diversity in communities across the nation through new and ongoing relationships with minority and women-owned businesses.

Lewis Brisbois is known for its commitment to principled advocacy, an unflinching work ethic, and unyielding recognition of our duty to provide the highest level of service to our clients, who choose us because we take the time to understand their business interests and internal culture. We have developed sophisticated proprietary risk evaluation and litigation management processes that many of our clients have incorporated into their business practices, and we help them manage and defend claims and litigation. As a result, they are avoiding and reducing losses that impact their bottom line.

Our practice includes pre-suit counseling and problem solving based on a structured and accurate analysis of likely outcome. We know our clients' objectives are often best served by a pre-suit resolution and we are often judged by the advice and counsel we provide toward that end. However, when trial is the answer and in the client's best interest, Lewis Brisbois brings to bear the full force of our tenacious and sophisticated litigation prowess, utilizing our nationwide network of attorneys and support staff as well as our considerable technological resources to achieve the best possible results for our clients.

LEWIS BRISBOIS LOCATIONS NATIONWIDE

Albuquerque, NM
Atlanta, GA
Baltimore, MD
Boston, MA
Charleston, WV
Chicago, IL
Cleveland, OH
Colorado Springs, CO
Dallas, TX
Denver, CO
Fort Lauderdale, FL
Fort Wright, KY
Hartford, CT
Houston, TX
Indian Wells, CA
Indianapolis, IN
Kansas City, MO
Lafayette, LA
Las Vegas, NV
Los Angeles, CA
Madison County, IL
Miami, FL
New Orleans, LA
New York, NY
Newark, NJ
Orange County, CA
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Providence, RI
Raleigh, NC
Sacramento, CA
San Bernardino, CA
San Diego, CA
San Francisco, CA
Seattle, WA
Tampa, FL
Temecula, CA
Tucson, AZ
Weirton, WV
Wichita, KS



LEWIS BRISBOIS BISGAARD & SMITH LLP

LewisBrisbois.com