



Since 1891

WE ARE NEW YORK'S LAW SCHOOL**A SPECIAL TWO-PART CLE SERIES****MORE DETAILS**

There will be an optional writing assignment for students who wish to have a cybersecurity writing sample.

2 CLE credits are available in Areas of Professional Practice (NY transitional and nontransitional).

The program is free; pizza will be served.

RSVP:
nyls.edu/BLIregister

MASTER CLASS**CYBER INCIDENT
RESPONSE PLANS:
THE "HOW-TO"
GUIDE FOR
LEGAL COUNSEL****Presenter: Lawrence Montle '13**

Chief Information Security and Privacy Officer,
New York State Insurance Fund

PART 1**Friday, October 12, 2018, 5:00 p.m.–7:00 p.m.**

Gain familiarity with the elements of an incident response plan required by the New York State Department of Financial Services. Work through a high-level review of a financial services incident response plan.

PART 2**Friday, October 26, 2018, 5:00 p.m.–7:00 p.m.**

Discuss the role of an incident response plan in cybersecurity. Work through a high-level review of a law firm incident response plan.



**Federal Deposit
Insurance Corporation**



[Home](#) > [Regulation & Examinations](#) > [Bank Examinations](#) > Supervisory Insights

Supervisory Insights

Incident Response Programs: Don't Get Caught Without One

Everyone is familiar with the old adage "Time is money." In the Information Age, data may be just as good. Reports of data compromises and security breaches at organizations ranging from universities and retail companies to financial institutions and government agencies provide evidence of the ingenuity of Internet hackers, criminal organizations, and dishonest insiders obtaining and profiting from sensitive customer information. Whether a network security breach compromising millions of credit card accounts or a lost computer tape containing names, addresses, and Social Security numbers of thousands of individuals, a security incident can damage corporate reputations, cause financial losses, and enable identity theft.

Banks are increasingly becoming prime targets for attack because they hold valuable data that, when compromised, may lead to identity theft and financial loss. This environment places significant demands on a bank's information security program to identify and prevent vulnerabilities that could result in successful attacks on sensitive customer information held by the bank. The rapid adoption of the Internet as a delivery channel for electronic commerce coupled with prevalent and highly publicized vulnerabilities in popular hardware and software have presented serious security challenges to the banking industry. In this high-risk environment, it is very likely that a bank will, at some point, need to respond to security incidents affecting its customers.

To mitigate the negative effects of security breaches, organizations are finding it necessary to develop formal incident response programs (IRPs).¹ However, at a time when organizations need to be most prepared, many banks are finding it challenging to assemble an IRP that not only meets minimum requirements (as prescribed by Federal bank regulators), but also provides for an effective methodology to manage security incidents for the benefit of the bank and its customers. In response to these challenges, this article highlights the importance of IRPs to a bank's information security program and provides information on required content and best practices banks may consider when developing effective response programs.

The Importance of an Incident Response Program

A bank's ability to respond to security incidents in a planned and coordinated fashion is important to the success of its information security program. While IRPs are important for many reasons, three are highlighted in this article.

First, though incident prevention is important, focusing solely on prevention may not be enough to insulate a bank from the effects of a security breach. Despite the industry's efforts at identifying and correcting security vulnerabilities, every bank is susceptible to weaknesses such as improperly configured systems, software vulnerabilities, and zero-day exploits.² Compounding the problem is the difficulty an organization experiences in sustaining a "fully secured" posture. Over the long term, a large amount of resources (time, money, personnel, and expertise) is needed to maintain security commensurate with all potential vulnerabilities. Inevitably, an organization faces a point of diminishing returns whereby the extra resources applied to incident prevention bring a lesser amount of security value. Even the best information security program may not identify every vulnerability and prevent every incident, so banks are best served by incorporating formal incident response planning to complement strong prevention measures. In the event management's efforts do not prevent all security incidents (for whatever reason), IRPs are necessary to reduce the sustained damage to the bank.

Second, regulatory agencies have recognized the value of IRPs and have mandated that certain incident response requirements be included in a bank's information security program. In March 2001, the FDIC, the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the Board of Governors of the Federal Reserve System (FRB) (collectively, the Federal bank regulatory agencies) jointly issued guidelines establishing standards for safeguarding customer information, as required by the Gramm-Leach-Bliley Act of 1999.³ These standards require banks to adopt response programs as a security measure. In April 2005, the Federal bank regulatory agencies issued interpretive guidance regarding response programs.⁴ This additional guidance describes IRPs and prescribes standard procedures that should be included in IRPs. In addition to Federal regulation in this area, at least 32 states have passed laws requiring that individuals be notified of a breach in the security of computerized personal information.⁵ Therefore, the increased regulatory attention devoted to incident response has made the development of IRPs a legal necessity.

Finally, IRPs are in the best interests of the bank. A well-developed IRP that is integrated into an overall information security program strengthens the institution in a variety of ways. Perhaps most important, IRPs help the bank contain the damage resulting from a security breach and lessen its downstream effect. Timely and decisive action can also limit the harm to the bank's reputation, reduce negative publicity, and help the bank identify and remedy the underlying causes of the security incident so that mistakes are not destined to be repeated.

Elements of an Incident Response Program

Although the specific content of an IRP will differ among financial institutions, each IRP should revolve around the minimum procedural requirements prescribed by the Federal bank regulatory agencies. Beyond this fundamental content, however, strong financial institution management teams also incorporate industry best practices to further refine and enhance their IRP. In general, the overall comprehensiveness of an IRP should be commensurate with an institution's administrative, technical, and organizational complexity.

Minimum Requirements

The minimum required procedures addressed in the April 2005 interpretive guidance can be categorized into two broad areas: "reaction" and "notification." In general, reaction procedures are the initial actions taken once a compromise has been identified. Notification procedures are relatively straightforward and involve communicating the details or events of the incident to interested parties; however, they may also involve some reporting requirements. Figure 1 lists the minimum required procedures of an IRP as discussed in the April 2005 interpretive guidance.

Figure 1

Minimum Requirements

Develop reaction procedures for

Establish notification procedures for

- | | |
|--|---|
| <ul style="list-style-type: none"> • assessing security incidents that have occurred; • identifying the customer information and information systems that have been accessed or misused; and | <ul style="list-style-type: none"> • the institution's primary Federal regulator; • appropriate law enforcement agencies (and filing Suspicious Activity Reports [SARs], if necessary); and |
|--|---|

- containing and controlling the security incident.
- affected customers.

Reaction Procedures

Assessing security incidents and identifying the unauthorized access to or misuse of customer information essentially involve organizing and developing a documented risk assessment process for determining the nature and scope of the security event. The goal is to efficiently determine the scope and magnitude of the security incident and identify whether customer information has been compromised.

Containing and controlling the security incident involves preventing any further access to or misuse of customer information or customer information systems. As there are a variety of potential threats to customer information, organizations should anticipate the ones that are more likely to occur and develop response and containment procedures commensurate with the likelihood of and the potential damage from such threats. An institution's information security risk assessment can be useful in identifying some of these potential threats. The containment procedures developed should focus on responding to and minimizing potential damage from the threats identified. Not every incident can be anticipated, but institutions should at least develop containment procedures for reasonably foreseeable incidents.

Notification Procedures

An institution should notify its primary Federal regulator as soon as it becomes aware of the unauthorized access to or misuse of sensitive customer information or customer information systems. Notifying the regulatory agency will help it determine the potential for broader ramifications of the incident, especially if the incident involves a service provider, as well as assess the effectiveness of the institution's IRP.

Institutions should develop procedures for notifying law enforcement agencies and filing SARs in accordance with their primary Federal regulator's requirements.⁶ Law enforcement agencies may serve as an additional resource in handling and documenting the incident. Institutions should also establish procedures for filing SARs in a timely manner because regulations impose relatively quick filing deadlines. The SAR form⁷ itself may serve as a resource in the reporting process, as it contains specific instructions and thresholds for when to file a report. The SAR form instructions also clarify what constitutes a "computer intrusion" for filing purposes. Defining procedures for notifying law enforcement agencies and filing SARs can streamline these notification and reporting requirements.

Institutions should also address customer notification procedures in their IRP. When an institution becomes aware of an incident involving unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to determine the likelihood that such information has been or will be misused. If the institution determines that sensitive customer information has been misused or that misuse of such information is reasonably possible, it should notify the affected customer(s) as soon as possible. Developing standardized procedures for notifying customers will assist in making timely and thorough notification. As a resource in developing these procedures, institutions should reference the April 2005 interpretive guidance, which specifically addresses when customer notification is necessary, the recommended content of the notification, and the acceptable forms of notification.

Best Practices—Going Beyond the Minimum

Each bank has the opportunity to go beyond the minimum requirements and incorporate industry best practices into its IRP. As each bank tailors its IRP to match its administrative, technical, and organizational complexity, it may find some of the following best practices relevant to its operating environment. The practices addressed below are not all inclusive, nor are they regulatory requirements. Rather, they are representative of some of the more effective practices and procedures some institutions have implemented. For organizational purposes, the best practices have been categorized into the various stages of incident response: preparation, detection, containment, recovery, and follow-up.

Preparation

Preparing for a potential security compromise of customer information is a proactive risk management practice. The overall effectiveness and efficiency of an organization's response is related to how well it has organized and prepared for potential incidents. Two of the more effective practices noted in many IRPs are addressed below.

• Establish an incident response team.

A key practice in preparing for a potential incident is establishing a team that is specifically responsible for responding to security incidents. Organizing a team that includes individuals from various departments or functions of the bank (such as operations, networking, lending, human resources, accounting, marketing, and audit) may better position the bank to respond to a given incident. Once the team is established, members can be assigned roles and responsibilities to ensure incident handling and reporting is comprehensive and efficient. A common responsibility that banks have assigned to the incident response team is developing a notification or call list, which includes contact information for employees, vendors, service providers, law enforcement, bank regulators, insurance companies, and other appropriate contacts. A comprehensive notification list can serve as a valuable resource when responding to an incident.

• Define what constitutes an incident.

An initial step in the development of a response program is to define what constitutes an incident. This step is important as it sharpens the organization's focus and delineates the types of events that would trigger the use of the IRP. Moreover, identifying potential security incidents can also make the possible threats seem more tangible, and thus better enable organizations to design specific incident-handling procedures for each identified threat.

Detection

The ability to detect that an incident is occurring or has occurred is an important component of the incident response process. This is considerably more important with respect to technical threats, since these can be more difficult to identify without the proper technical solutions in place. If an institution is not positioned to quickly identify incidents, the overall effectiveness of the IRP may be affected.⁸ Following are two detection-related best practices included in some institutions' IRPs.

• Identify indicators of unauthorized system access.

Most banks implement some form of technical solution, such as an intrusion detection system or a firewall, to assist in the identification of unauthorized system access. Activity reports from these and other technical solutions (such as network and application security reports) serve as inputs for the monitoring process and for the IRP in general. Identifying potential indicators of unauthorized system access within these activity or security reports can assist in the detection process.

• Involve legal counsel.

Because many states have enacted laws governing notification requirements for customer information security compromises, institutions have found it prudent to involve the institution's legal counsel when a compromise of customer information has been detected. Legal guidance may also be warranted in properly documenting and handling the incident.

Containment

During the containment phase, the institution should generally implement its predefined procedures for responding to the specific incident (note that containment procedures are a required minimum component). Additional containment-related procedures some banks have successfully incorporated into their IRPs are discussed below.

• Establish notification escalation procedures.

If senior management is not already part of the incident response team, banks may want to consider developing procedures for notifying these individuals when the situation warrants. Providing the appropriate executive staff and senior department managers with information about how containment actions will affect business operations or systems and including these individuals in the decision-making process can help minimize undesirable business disruptions. Institutions that have

experienced incidents have generally found that the management escalation process (and resultant communication flow) was not only beneficial during the containment phase, but also proved valuable during the later phases of the incident response process.

- **Document details, conversations, and actions.**

Retaining documentation is an important component of the incident response process. Documentation can come in a variety of forms, including technical reports generated, actions taken, costs incurred, notifications provided, and conversations held. This information may be useful to external consultants and law enforcement for investigative and legal purposes, as well as to senior management for filing potential insurance claims and for preparing an executive summary of the events for the board of directors or shareholders. In addition, documentation can assist management in responding to questions from its primary Federal regulator. It may be helpful during the incident response process to centralize this documentation for organizational purposes.

- **Organize a public relations program.**

Whether a bank is a local, national, or global firm, negative publicity about a security compromise is a distinct possibility. To address potential reputation risks associated with a given incident, some banks have organized public relations programs and designated specific points of contact to oversee the program. A well-defined public relations program can provide a specific avenue for open communications with both the media and the institution's customers.

Recovery

Recovering from an incident essentially involves restoring systems to a known good state or returning processes and procedures to a functional state. Some banks have incorporated the following best practices related to the recovery process in their IRPs.

- **Determine whether configurations or processes should be changed.**

If an institution is the subject of a security compromise, the goals in the recovery process are to eliminate the cause of the incident and ensure that the possibility of a repeat event is minimized. A key component of this process is determining whether system configurations or other processes should be changed. In the case of technical compromises, such as a successful network intrusion, the IRP can prompt management to update or modify system configurations to help prevent further incidents. Part of this process may include implementing an effective, ongoing patch management program, which can reduce exposure to identified technical vulnerabilities. In terms of non-technical compromises, the IRP can direct management to review operational procedures or processes and implement changes designed to prevent a repeat incident.

- **Test affected systems or procedures prior to implementation.**

Testing is an important function in the incident response process. It helps ensure that reconfigured systems, updated procedures, or new technologies implemented in response to an incident are fully effective and performing as expected. Testing can also identify whether any adjustments are necessary prior to implementing the updated system, process, or procedure.

Follow-up

During the follow-up process, an institution has the opportunity to regroup after the incident and strengthen its control structure by learning from the incident. A number of institutions have included the following best practice in their IRPs.

- **Conduct a "lessons-learned" meeting.**

Successful organizations can use the incident and build from the experience. Organizations can use a lessons-learned meeting to

- discuss whether affected controls or procedures need to be strengthened beyond what was implemented during the recovery phase;
- discuss whether significant problems were encountered during the incident response process and how they can be addressed;
- determine if updated written policies or procedures are needed for the customer information security risk assessment and information security program;
- determine if updated training is necessary regarding any new procedures or updated policies that have been implemented; and
- determine if the bank needs additional personnel or technical resources to be better prepared going forward.

The preceding best practices focused on the more common criteria that have been noted in actual IRPs, but some banks have developed other effective incident response practices. Examples of these additional practices are listed in Figure 2. Organizations may want to review these practices and determine if any would add value to their IRPs given their operating environments.

Figure 2

Additional IRP Best Practices

- Test the incident response plan (via walkthrough or tabletop exercises) to assess thoroughness.
- Implement notices on login screens for customer information systems to establish a basis for disciplinary or legal action.
- Develop an incident grading system that quantifies the severity of the incident, helps determine if the incident response plan needs to be activated, and specifies the extent of notification escalation.
- Provide periodic staff awareness training on recognizing potential indicators of unauthorized activity and reporting the incident through proper channels. Some institutions have established phone numbers and e-mail distribution lists for reporting possible incidents.
- Inform users about the status of any compromised system they may be using.
- Establish a list of possible consultants, in case the bank does not have the expertise to handle or investigate the specific incident (especially regarding technical compromises).
- Establish evidence-gathering and handling procedures aimed at preserving evidence of the incident and aiding in prosecution activities.

What the Future Holds

In addition to meeting regulatory requirements and addressing applicable industry best practices, several characteristics tend to differentiate banks. The most successful banks will find a way to integrate incident response planning into normal operations and business processes. Assimilation efforts may include expanding security awareness and training initiatives to reinforce incident response actions, revising business continuity plans to incorporate security incident responses, and implementing additional security monitoring systems and procedures to provide timely incident notification. Ultimately, the adequacy of a bank's IRP reflects on the condition of the information security program along with management's willingness and ability to manage information technology risks. In essence, incident response planning is a management process, the comprehensiveness and success of which provide insight into the quality and attentiveness of management. In

this respect, the condition of a bank's IRP, and the results of examiner review of the incident response planning process, fit well within the objectives of the information technology examination as described in the Information Technology–Risk Management Program.⁹

An IRP is a critical component of a well-formed and effective information security program and has the potential to provide tangible value and benefit to a bank. Similar to the importance of a business continuity planning program as it relates to the threat of natural and man-made disasters, sound IRPs will be necessary to combat new and existing data security threats facing the banking community. Given the high value placed on the confidential customer information held within the financial services industry, coupled with the publicized success of known compromises, one can reasonably assume that criminals will continue to probe an organization's defenses in search of weak points. The need for response programs is real and has been recognized as such by not only state and Federal regulatory agencies (through passage of a variety of legal requirements), but by the banking industry itself. The challenges each bank faces are to develop a reasonable IRP providing protections for the bank *and* the consumer and to incorporate the IRP into a comprehensive, enterprise-wide information security program. The most successful banks will exceed regulatory requirements to leverage the IRP for business advantages and, in turn, improved protection for the banking industry as a whole.

Eric R. Morris

Information Technology Examiner, Chicago, IL

John J. Sosnowski II

Examiner, Indianapolis, IN

¹In its simplest form, an IRP is an organized approach to addressing and managing the aftermath of a security breach or attack.

²A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

³Appendix B to Part 364 of the FDIC Rules and Regulations at www.fdic.gov/regulations/laws/rules/2000-8660.html#2000appendixbtopart364 and FDIC FIL-22-2001, Guidelines Establishing Standards for Safeguarding Customer Information, issued March 14, 2001. Also refer to 12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (FRB); and 12 CFR 570, App. B (OTS).

⁴FDIC FIL-27-2005, Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued April 1, 2005, www.fdic.gov/news/news/financial/2005/fil2705.html. Also refer to 12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (FRB); 12 CFR 364, App. B (FDIC); and 12 CFR 570, App. B (OTS).

⁵"State Security Breach Notification Laws (as of June 2006)," September 15, 2006, www.thecyberangel.com/StSecBrchNotifLaw.doc.

⁶An institution's obligation to file a SAR is specified in the regulations of its primary Federal regulator. Refer to 12 CFR 21.11 (OCC), 12 CFR 208.62 (FRB), 12 CFR 353 (FDIC), and 12 CFR 563.180 (OTS).

⁷See www.fincen.gov/reg_bsaforms.html.

⁸Pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the FDIC, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission, have jointly proposed (1) guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft, and (2) regulations requiring each financial institution and creditor to establish reasonable policies and procedures for implementing the guidelines. The notice of proposed rulemaking (NPR) also includes provisions requiring credit and debit card issuers to assess the validity of a request for a change of address under certain circumstances, and, pursuant to section 315 of the FACT Act, guidance regarding reasonable policies and procedures that a user of consumer reports must employ when such a user receives a notice of address discrepancy from a consumer reporting agency. The NPR was published on July 18, 2006, at 71 Fed. Reg. 40786, and the comment period ended on September 18, 2006. The agencies are reviewing the comments received in preparation for a final rule.

⁹The Information Technology–Risk Management Program (IT–RMP) is the approach for conducting information technology examinations at FDIC-supervised institutions, regardless of size and complexity. FIL 81-2005, Information Technology–Risk Management Program New Information Technology Examination Procedures, August 18, 2005, www.fdic.gov/news/news/financial/2005/fil8105.html.

[Table of Contents](#)

Last Updated 12/14/2006

SupervisoryJournal@fdic.gov

[Home](#) [Contact Us](#) [Search](#) [Help](#) [SiteMap](#) [Forms](#) [En Español](#)

[Website Policies](#) [Privacy Policy](#) [Accessibility Statement](#) [Plain Writing Act of 2010](#) [USA.gov](#) [FDIC Office of Inspector General](#)

[Freedom of Information Act \(FOIA\) Service Center](#) [FDIC Open Government Webpage](#) [No FEAR Act Data](#)



Search

Franchise Process Opportunities Vendor Info

- Cybersecurity Requirements for Vendors & Contractors
- Technical Vendor Resources
- Contractual Authority & Adding Additional Terms

Cybersecurity Requirements for Vendors & Contractors

DoITT is responsible for publishing Citywide Cybersecurity Policies and Standards, of which all City agencies, employees, contractors, and vendors are required to follow. This page contains those policies which have been classified as public information.

The City of New York takes our charge to protect the personally identifiable information that we collect while providing municipal services to the public very seriously. All employees and contractors with access to City information systems are required to read and acknowledge the User Responsibilities policy prior to accessing any City information systems.

- Anti-Piracy
- Anti-Virus
- Change Management
- CISO Role
- Data Classification
- Digital Media Re-use and Disposal Policy
- Encryption
- External Identity Management And Password
- Identity Management
- Logon Banner
- Mobile Computing Device Security
- Password
- Personnel
- Portable Data
- Remote Access
- Security Architecture Standard
- Service Provider Policy

- Application Security Policy
- User Responsibilities
- Vulnerability Management
- Wireless Security

**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 non-governmental 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.

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:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

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

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

- (j) physical security and environmental controls;
- (k) customer data privacy;
- (l) vendor and Third Party Service Provider management;
- (m) risk assessment; and
- (n) 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.

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:

(a) 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

(b) 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.

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

(a) 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

(b) 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 under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) 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.

(e) 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 within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) 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.

APPENDIX A (Part 500)

(Covered Entity Name)

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ____.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____

Date: _____

[DFS Portal Filing Instructions]

APPENDIX B (Part 500)

(Covered Entity Name)

(Date)_____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____

Date: _____

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]

[Home](#)[ABOUT US](#)[Consumers](#)[Banking Industry](#)[Insurance Industry](#)[Legal](#)[Reports & Publications](#)[Mission & Leadership](#)[Initiatives](#)[History](#)[News Room](#)[Who We Supervise](#)[Careers with DFS](#)[Contact Us](#)[Procurement](#)

FREQUENTLY ASKED QUESTIONS REGARDING 23 NYCRR PART 500

Effective March 1, 2017, the Superintendent of Financial Services promulgated **23 NYCRR Part 500**, a regulation establishing cybersecurity requirements for financial services companies. The following provides answers to frequently asked questions concerning 23 NYCRR Part 500. Terms used below have the meanings assigned to them in 23 NYCRR 500.01. Please note that the Department may revise or update the below information from time to time, as appropriate.

1. Are Exempt Mortgage Servicers Covered Entities under 23 NYCRR 500?

Under N.Y. Bank Law § 590(2)(b-1), an exempt entity will need to prove its "exempt organization" status. Since the notification is not an authorization from the Department, an Exempt Mortgage Servicer, under N.Y. Bank Law § 590(2)(b-1), will not fit the definition of a Covered Entity under 500.01(c). However, Exempt Mortgage Loan Servicers that also hold a license, registration, or received approval under the provisions of Part 418.2(e) are required to prove exemption and comply with regulation. With respect to DFS's cybersecurity regulation, given the ever-increasing cybersecurity risks that financial institutions face, DFS strongly encourages all financial institutions, including exempt Mortgage Servicers, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

2. Are Not-for-profit Mortgage Brokers Covered Entities under 23 NYCRR 500?

Yes. Not-for-profit Mortgage Brokers are Covered Entities under 23 NYCRR 500. 3 NYCRR Part 39.4(e) provides that Mortgage Brokers "which seek exemption may submit a letter application" to the Mortgage Banking unit of the Department at the address set forth in section 1.1 of Supervisory Policy G 1, "together with such information as may be prescribed by" the Superintendent. As this authorization is necessary for a Not-for-profit Mortgage Broker, it is a Covered Entity under 23 NYCRR 500.

3. Do Covered Entities have any obligations when acquiring or merging with a new company?

Section 500.09(a) states that the "Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations." Furthermore, Section 500.08(b) states that the institution's application security "procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity." As such, when Covered Entities are acquiring or merging with a new company, Covered Entities will need to do a factual analysis of how these regulatory requirements apply to that particular acquisition. Some important considerations include, but are not limited to, what business the acquired company engages in, the target company's risk for cybersecurity including its availability of PII, the safety and soundness of the Covered Entity, and the integration of data systems. The Department emphasizes that Covered Entities need to have a serious due diligence process and cybersecurity should be a priority when considering any new acquisitions.

4. Are Health Maintenance Organizations (HMOs) and continuing care retirement communities (CCRCs) Covered Entities?

Yes. Both HMOs and CCRCs are Covered Entities. Pursuant to the Public Health Law, HMOs must receive authorization and prior approval of the forms they use and the rates they charge for comprehensive health insurance in New York. The Public Health Law subjects HMOs to DFS authority by making provisions of the Insurance Law applicable to them. CCRCs are required by Insurance Law Section 1119 to have contracts and rates reviewed and authorized by DFS. The Public Health Law also subjects HMOs and CCRCs to the examination authority of the Department. As this authorization is fundamental to the ability to conduct their businesses, HMOs and CCRCs are Covered Entities because they are "operating under or required to operate under" DFS authorizations pursuant to the Insurance Law. Moreover, since these entities have sensitive, private data, their compliance with cybersecurity protection is necessary.

5. Assuming there is no continuous monitoring under 23 NYCRR Section 500.05, does the Department require that a Covered Entity complete a Penetration Test and vulnerability assessments by March 1, 2018?

The Regulation requires Covered Entities to have a plan in place that provides for Penetration Testing to be done as appropriate to address the risks of the Covered Entity. Such plan must encompass Penetration Testing at least annually and bi-annual vulnerability assessments, but the first annual Penetration Testing and first vulnerability assessment need not have been concluded before March 1, 2018 under Section 500.05. The Department expects all institutions with no continuous monitoring to complete robust Penetration Testing and vulnerability assessment in a timely manner as they are a crucial component of a cybersecurity program.

6. If Covered Entity A utilizes Covered Entity B (not related to Covered Entity A) as a Third Party Service Provider, and Covered Entity B provides Covered Entity A with evidence of its Certification of Compliance with NYSDFS Cybersecurity Regulations, could that be considered adequate due diligence under the due diligence process required by Section 500.11(a)(3)?

No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019.

7. Does a Covered Entity need to amend its Notice of Exemption in the event of changes after the initial submission (e.g., name changes or changes to the applicable exemption(s))?

If there are changes, the Covered Entity should submit a new Notice of Exemption, which would not be considered an amendment to the original submission. For example, if a Covered Entity originally submitted a Notice of Exemption stating that it qualified for exemptions under Sections 500.19(b) and 500.19(a)(1), but it now only qualifies for a Section 500.19(a)(1) exemption, then the Covered Entity must submit a new Notice of Exemption with the correct information.

The Department also emphasizes that Notices of Exemption should be filed electronically via the DFS Web Portal <http://www.dfs.ny.gov/about/cybersecurity>. The Covered Entity should utilize the account that they used to file the original Notice of Exemption or create a new account if an individual filing was previously not made. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

8. Should a Covered Entity send supporting documentation along with the Certification of Compliance?

The Covered Entity must submit the compliance certification to the Department and is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the regulation. The Department also expects that the Covered Entity maintains the documents and records necessary that support the certification, should the Department request such information in the future. Likewise, under 23 NYCRR Section 500.17, to the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity must document such efforts and maintain such schedules and documentation for inspection during the examination process or as otherwise requested by the Department.

9. Is a Covered Entity entitled to an exemption under Section 500.19(b) if that Covered Entity is an employee, agent, representative or designee of more than one other Covered Entity?

Section 500.19(b) states that a Covered Entity who is an "employee, agent, representative or designee of a Covered Entity . . . is exempt from" 23 NYCRR Part 500 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" (emphasis added). This exemption requires an entire employee, agent, representative or designee to be fully covered by the program of another Covered Entity. Therefore, a Covered Entity who is an employee, agent, representative or designee of more than one other Covered Entity will only qualify for a Section 500.19(b) exemption where the cybersecurity program of at least one of its parent Covered Entities fully covers all aspects of the employee's, agent's, representative's or designee's business.

10. Does a Covered Entity that qualifies for an exemption under 23 NYCRR Section 500.19(b) need to file a notice of exemption?

Yes. 23 NYCRR 500.19 subsections (a) through (d) set forth certain limited exemptions from different requirements of Part 500. Pursuant to 23 NYCRR Section 500.19(e): "[a] Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption" (emphasis added).

11. Under Section 500.04(b), can the requirement that the CISO report in writing at least annually "to the Covered Entity's board of directors" (the "board") be met by reporting to an authorized subcommittee of the board?

No. The Department emphasizes that a well-informed board is a crucial part of an effective cybersecurity program and the CISO's reporting to the full board is important to enable the board to assess the Covered Entity's governance, funding, structure and effectiveness as well as compliance with 23 NYCRR Part 500 or other applicable laws or regulations.

12. Can a Covered Entity file a notice of exemption on behalf of its employees or agents?

By permission, the Department will approve certain Covered Entities to file notices of exemption on behalf of their employees or captive agents who are also Covered Entities. This option will only be available for filings of 50 or more employees or captive agents and only if all employees or captive agents qualify for the same exemptions. Covered Entities with over 50 employees or agents on whose behalf they have authority to file should contact the Department at CyberRegComments@dfs.ny.gov from the email to which your Cybersecurity portal account is associated with the [following instructions](#). The Department will coordinate with the Covered Entity to submit a one-time filing form to effectuate an exemption filing for multiple covered entities. On the spreadsheet, the submitter will need to provide the first and last name, DFS identification number, type of license, and email for every employee or captive agent. After approval, the Department will send more detailed instructions and the exemption spreadsheet. In the event that there is a need for additional names or captive agents after the initial submission, the submitter will be able to submit a supplemental form through the portal. The Department emphasizes that the employee or captive agent, for whom the Covered Entity is filing, continues to be ultimately responsible in ensuring compliance with 23 NYCRR Part 500. It remains the responsibility of the employee or captive agent to notify the Department of any changes in their status.

13. When is an unsuccessful attack a Cybersecurity Event that has or had "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" under the reporting requirements of 23 NYCRR Section

500.17(a)(2)?

The Department recognizes that Covered Entities 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 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.

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.

14. Are the New York branches of out-of-state domestic banks required to comply with 23 NYCRR Part 500?

New York is a signatory to the Nationwide Cooperative Agreement, Revised as of December 9, 1997 (the "Agreement"), an agreement among state banking regulators that addresses supervision in an interstate branching environment. Pursuant to the Agreement, the home state of a state-chartered bank with a branch or branches in New York under Article V-C of the New York Banking Law is primarily responsible for supervising such state-chartered bank, including its New York branches. In keeping with the Agreement's goals of interstate coordination and cooperation with respect to the supervision and examination of bank branches, including compliance with applicable laws, DFS will defer to the home state supervisor for supervision and examination of the New York branches, with the understanding that DFS is available to coordinate and work with the home state in such supervision and examination. DFS notes that New York branches are required to comply with New York state law, and DFS maintains the right to examine branches located in New York. With respect to DFS's cybersecurity regulation, given the ever-increasing cybersecurity risks that financial institutions face, DFS strongly encourages all financial institutions, including New York branches of out-of-state domestic banks, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

15. How must a Covered Entity address cybersecurity issues with respect to its subsidiaries and other affiliates?

When a subsidiary or other affiliate of a Covered Entity presents risks to the Covered Entity's Information Systems or the Nonpublic Information stored on those Information Systems, those risks must be evaluated and addressed in the Covered Entity's Risk Assessment, cybersecurity program and cybersecurity policies (see 23 NYCRR Sections 500.09, 500.02 and 500.03, respectively). Other regulatory requirements may also apply, depending on the individual facts and circumstances.

16. If a Covered Entity qualifies for a limited exemption, does it need to comply with 23 NYCRR Part 500?

The exemptions listed in 23 NYCRR Part 500.19 are limited in scope. These exemptions have been tailored to address particular circumstances and include requirements that the Department believes are necessary for these exempted entities. As such, Covered Entities that qualify for those exemptions are only exempt from complying with certain provisions as set forth in the regulation, but must comply with the sections listed in the exemption that applies to that Covered Entity.

17. Under 23 NYCRR 500.17(a), is a Covered Entity required to give notice to the Department when a Cybersecurity Event involves harm to consumers?

Yes. 23 NYCRR 500.17(a) must be read in combination with other laws and regulations that apply to consumer privacy. Under 23 NYCRR 500.17(a)(1), a Covered Entity must give notice to the Department of any Cybersecurity Event "of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body," which includes many Cybersecurity Events that involve consumer harm, whether actual or potential. To offer just one example, New York's information security breach and notification law requires notices to affected consumers and to certain government bodies following a data breach. Under 23 NYCRR 500.17(a)(1), when such a data breach constitutes a Cybersecurity Event, it must also be reported to the Department.

In addition, under 23 NYCRR 500.17(a)(2), Cybersecurity Events must be reported to the Department if they "have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." To the extent a Cybersecurity Event involves material consumer harm, it is covered by this provision.

18. Is a Covered Entity required to give notice to consumers affected by a Cybersecurity Event?

New York's information security breach and notification law (General Business Law Section 899-aa), requires notice to consumers who have been affected by cybersecurity incidents. Further, under 23 NYCRR Part 500, a Covered Entity's cybersecurity program

and policy must address, to the extent applicable, consumer data privacy and other consumer protection issues. Additionally, Part 500 requires that Covered Entities address as part of their incident response plans external communications in the aftermath of a breach, which includes communication with affected customers. Thus, a Covered Entity's cybersecurity program and policies will need to address notice to consumers in order to be consistent with the risk-based requirements of 23 NYCRR Part 500.

19. May a Covered Entity adopt portions of an Affiliate's cybersecurity program without adopting all of it?

A Covered Entity may adopt an Affiliate's cybersecurity program in whole or in part, as long as the Covered Entity's overall cybersecurity program meets all requirements of 23 NYCRR Part 500. The Covered Entity remains responsible for full compliance with the requirements of 23 NYCRR Part 500. To the extent a Covered Entity relies on an Affiliate's cybersecurity program in whole or in part, that program must be made available for examination by the Department.

20. May the certification requirement of 23 NYCRR 500.17(b) be met by an Affiliate?

No. Each Covered Entity is required to annually certify its compliance with Part 500 as required by 23 NYCRR 500.17(b).

21. To the extent a Covered Entity uses an employee of an Affiliate as its Chief Information Security Officer ("CISO"), is the Covered Entity required to satisfy the requirements of 23 NYCRR 500.04(a)(2)-(3)?

To the extent a Covered Entity utilizes an employee of an Affiliate to serve as the Covered Entity's CISO for purposes of 23 NYCRR 500.04(a), the Affiliate is not considered a Third Party Service Provider for purposes of 23 NYCRR 500.04(a)(2)-(3). However, the Covered Entity retains full responsibility for compliance with the requirements of 23 NYCRR Part 500 at all times, including ensuring that the CISO responsible for the Covered Entity is performing the duties consistent with this Part.

22. Are the DFS-authorized New York branches, agencies and representative offices of out-of-country foreign banks required to comply with 23 NYCRR Part 500?

Yes. It is further noted that, in such cases, only the Information Systems supporting the branch, agency or representative office, and the Nonpublic Information of the branch, agency or representative office are subject to the applicable requirements of 23 NYCRR Part 500, whether through the branch's, agency's or representative office's development and implementation of its own cybersecurity program or through the adoption of an Affiliate's cybersecurity program.

23. Where interrelated requirements under 23 NYCRR Part 500 are subject to different transitional periods, when and to what extent are Covered Entities required to comply with currently applicable requirements that are impacted by separate requirements for which the applicable transitional period has not yet ended?

Covered Entities have 180 days from the March 1, 2017, effective date to come into compliance with the requirements of 23 NYCRR Part 500 unless otherwise specified in 23 NYCRR 500.22. While complying with currently applicable requirements under the final rule, Covered Entities are generally not required to comply with, or incorporate into their cybersecurity programs, provisions of the regulation for which the applicable transitional period has not yet ended. For example, while Covered Entities will be required to have a cybersecurity program as well as policies and procedures in place by August 28, 2017, the Department recognizes that in some cases there may be updates and revisions thereafter that incorporate the results of a Risk Assessment later conducted, or other elements of Part 500 that are subject to longer transitional periods.

24. Is a Covered Entity required to certify compliance with all the requirements of 23 NYCRR 500 on February 15, 2018?

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.

25. 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 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 considered applicable for purposes of a certification under 23 NYCRR 500.17(b).

26. What constitutes "continuous monitoring" for purposes of 23 NYCRR 500.05?

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.

27. When is a Covered Entity required to report a Cybersecurity Event under 23 NYCRR 500.17(a)?

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.

28. How should a Covered Entity submit Notices of Exemption, Certifications of Compliance and Notices of Cybersecurity Events?

Cybersecurity Notices of Exemption, Certifications of Compliance, and Notices of Cybersecurity Events should be filed electronically via the DFS Web Portal <http://www.dfs.ny.gov/about/cybersecurity>. You will first be prompted to create an account and log in to the DFS Web Portal, then directed to the filing interface. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

29. Can an entity be both a Covered Entity and a Third Party Service Provider under 23 NYCRR Part 500?

Yes. If an entity is both a Covered Entity and a Third Party Service Provider, the entity is responsible for meeting the requirements of 23 NYCRR Part 500 as a Covered Entity.

30. Are all Third Party Service Providers required to implement Multi-Factor Authentication and encryption when dealing with a Covered Entity?

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.

Updated 02/23/2018

Department of Financial Services

Consumer Quicklinks

File a Complaint
Obtain a Lien Release on a Car
File a FOIL Request
Learn about Tenant's Rights
File an External Appeal
Report Fraud
DMV Insurance Codes

Industry Quicklinks

Check Insurance License Status
Serve Process
File a 90-Day Foreclosure Notice
Get Approval for a Title
Report Fraud
Independent Adjusters

Website

Accessibility
Disclaimer
Privacy Policy
Site Map
PDF Reader

Language Assistance

Español (Spanish)
中文 (Chinese)
Русский (Russian)
Italiano (Italian)
Kreyòl ayisyen (Haitian-Creole)
한국어 (Korean)
Polski (Polish)

CONNECT WITH US

DFS Secure Portal



REGISTER TO VOTE

Sign up online or download and mail in your application.

REGISTER NOW

Law firm incident response plan

- 1) The person who discovers the incident will email Bill and cc Security within three business days. For contact information see Appendix D.
- 2) If the person discovering the incident is a member of the IT department or affected department, if it is after 9 the Managing Partner should not be emailed or called, proceed to step 5.
- 3) Contact significant clients of the firm and explain the problem.
- 4) The person who discovered the issue shall documents the breach for the record. The grounds security office will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The grounds security office will log:
- 5) The IT staff member or affected department staff member who receives the (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could possibly add the following:
 - a) Is the equipment affected business critical?
 - b) What is the severity of the potential impact?
 - c) Name of system being targeted, along with operating system, IP address, and location.
 - d) IP address and any information about the origin of the attack.
- 6) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
- 7) Questions for the incident first responder:
 - a) Is the incident real or perceived?
 - (1) Has the incident been verified or is it a false positive.
 - b) When was the incident discovered?
 - c) By whom was the incident discovered?
 - (1) By internal staff
 - (2) By an external party
 - (a) Reported by a vendor
 - (b) Reported by law enforcement (FBI, Secret Service)
 - (c) Reported by the press.

- d) Is the incident still in progress?
 - e) What data or property is threatened and how critical is it?
 - f) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
 - g) What system or systems are targeted, where are they located physically and on the network?
 - h) Is the incident inside the trusted network?
 - i) Is the response urgent?
 - j) Can the incident be quickly contained?
 - k) Will the response alert the attacker and compromise the response?
 - l) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.
- 8) An incident ticket will be created. The incident will be categorized into the of one of the following categories:
- a) High- critical
 - b) Low- unimportant
- 9) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible.
- 10) Team members will work together to determine the best process to handle any incident.
- The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.
- 11) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
- 12) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
- 13) Upon management approval, the changes will be implemented.
- 14) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
- a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
 - b) Make users change passwords if passwords may have been sniffed.

- c) Be sure the system has been hardened by turning off or uninstalling unused services.
 - d) Be sure the system is fully patched.
 - e) Be sure real time virus protection and intrusion detection is running.
 - f) Be sure the system is logging the correct events and to the proper level.
- 15) Documentation—the following shall be documented:
- a) How the incident was discovered.
 - b) The category of the incident.
 - c) How the incident occurred, whether through email, firewall, etc.
 - d) Where the attack came from, such as IP addresses and other related information about the attacker.
 - e) What the response plan was.
 - f) What was done in response?
 - g) Whether the response was effective.
- 16) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
- 17) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
- 18) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
- a) Consider whether an additional policy could have prevented the intrusion.
 - b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
 - c) Was the incident response appropriate? How could it be improved?
 - d) Was every appropriate party informed in a timely manner?
 - e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
 - f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
 - g) Have changes been made to prevent a new and similar infection?
 - h) Should any security policies be updated?
 - i) What lessons have been learned from this experience?

Appendix A.

Contact list

Information Technology	Bill Tech	BTech@alawfirm.com
Legal	Susan DeMall	SDeMall@alawfirm.com
Human Resources	Thomas Persons	TPersons@alawfirm.com
Building Security	Acme Security	Guards@acme security

Creation date-4/10/2014

Last edited date – 4/11/2014

Approval date-



**National Institute of
Standards and Technology**
U.S. Department of Commerce

**Special Publication 800-61
Revision 2**

Computer Security Incident Handling Guide

**Recommendations of the National Institute
of Standards and Technology**

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

Table of Contents

Executive Summary	1
1. Introduction	4
1.1 Authority	4
1.2 Purpose and Scope	4
1.3 Audience	4
1.4 Document Structure	4
2. Organizing a Computer Security Incident Response Capability	6
2.1 Events and Incidents	6
2.2 Need for Incident Response	6
2.3 Incident Response Policy, Plan, and Procedure Creation	7
2.3.1 Policy Elements	7
2.3.2 Plan Elements	8
2.3.3 Procedure Elements	8
2.3.4 Sharing Information With Outside Parties	9
2.4 Incident Response Team Structure	13
2.4.1 Team Models	13
2.4.2 Team Model Selection	14
2.4.3 Incident Response Personnel	16
2.4.4 Dependencies within Organizations	17
2.5 Incident Response Team Services	18
2.6 Recommendations	19
3. Handling an Incident	21
3.1 Preparation	21
3.1.1 Preparing to Handle Incidents	21
3.1.2 Preventing Incidents	23
3.2 Detection and Analysis	25
3.2.1 Attack Vectors	25
3.2.2 Signs of an Incident	26
3.2.3 Sources of Precursors and Indicators	27
3.2.4 Incident Analysis	28
3.2.5 Incident Documentation	30
3.2.6 Incident Prioritization	32
3.2.7 Incident Notification	33
3.3 Containment, Eradication, and Recovery	35
3.3.1 Choosing a Containment Strategy	35
3.3.2 Evidence Gathering and Handling	36
3.3.3 Identifying the Attacking Hosts	37
3.3.4 Eradication and Recovery	37
3.4 Post-Incident Activity	38
3.4.1 Lessons Learned	38
3.4.2 Using Collected Incident Data	39
3.4.3 Evidence Retention	41
3.5 Incident Handling Checklist	42
3.6 Recommendations	42
4. Coordination and Information Sharing	45

4.1	Coordination	45
4.1.1	Coordination Relationships	46
4.1.2	Sharing Agreements and Reporting Requirements	47
4.2	Information Sharing Techniques	48
4.2.1	Ad Hoc	48
4.2.2	Partially Automated	48
4.2.3	Security Considerations	49
4.3	Granular Information Sharing	49
4.3.1	Business Impact Information	49
4.3.2	Technical Information	50
4.4	Recommendations	51

List of Appendices

Appendix A— Incident Handling Scenarios	52
A.1 Scenario Questions	52
A.2 Scenarios	53
Appendix B— Incident-Related Data Elements	58
B.1 Basic Data Elements	58
B.2 Incident Handler Data Elements	59
Appendix C— Glossary	60
Appendix D— Acronyms	61
Appendix E— Resources	63
Appendix F— Frequently Asked Questions	65
Appendix G— Crisis Handling Steps	68
Appendix H— Change Log	69

List of Figures

Figure 2-1. Communications with Outside Parties	10
Figure 3-1. Incident Response Life Cycle	21
Figure 3-2. Incident Response Life Cycle (Detection and Analysis)	25
Figure 3-3. Incident Response Life Cycle (Containment, Eradication, and Recovery)	35
Figure 3-4. Incident Response Life Cycle (Post-Incident Activity)	38
Figure 4-1. Incident Response Coordination	46

Executive Summary

Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. To that end, this publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential. Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement).

This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This revision of the publication, Revision 2, updates material throughout the publication to reflect the changes in attacks and incidents. Understanding threats and identifying modern attacks in their early stages is key to preventing subsequent compromises, and proactively sharing information among organizations regarding the signs of these attacks is an increasingly effective way to identify them.

Implementing the following requirements and recommendations should facilitate efficient and effective incident response for Federal departments and agencies.

Organizations must create, provision, and operate a formal incident response capability. Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS).

The Federal Information Security Management Act (FISMA) requires Federal agencies to establish incident response capabilities. Each Federal civilian agency must designate a primary and secondary point of contact (POC) with US-CERT and report all incidents consistent with the agency's incident response policy. Each agency is responsible for determining how to fulfill these requirements.

Establishing an incident response capability should include the following actions:

- Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide

- Staffing and training the incident response team.

Organizations should reduce the frequency of incidents by effectively securing networks, systems, and applications.

Preventing problems is often less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important complement to an incident response capability. If security controls are insufficient, high volumes of incidents may occur. This could overwhelm the resources and capacity for response, which would result in delayed or incomplete recovery and possibly more extensive damage and longer periods of service and data unavailability. Incident handling can be performed more effectively if organizations complement their incident response capability with adequate resources to actively maintain the security of networks, systems, and applications. This includes training IT staff on complying with the organization's security standards and making users aware of policies and procedures regarding appropriate use of networks, systems, and applications.

Organizations should document their guidelines for interactions with other organizations regarding incidents.

During incident handling, the organization will need to communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and victim organizations. Because these communications often need to occur quickly, organizations should predetermine communication guidelines so that only the appropriate information is shared with the right parties.

Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident. This publication defines several types of incidents, based on common attack vectors; these categories are not intended to provide definitive classification for incidents, but rather to be used as a basis for defining more specific handling procedures. Different types of incidents merit different response strategies. The attack vectors are:

- **External/Removable Media:** An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
- **Web:** An attack executed from a website or web-based application.
- **Email:** An attack executed via an email message or attachment.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.
- **Other:** An attack that does not fit into any of the other categories.

Organizations should emphasize the importance of incident detection and analysis throughout the organization.

In an organization, millions of possible signs of incidents may occur each day, recorded mainly by logging and computer security software. Automation is needed to perform an initial analysis of the data and select events of interest for human review. Event correlation software can be of great value in automating the analysis process. However, the effectiveness of the process depends on the quality of the data that goes into it. Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.

Organizations should create written guidelines for prioritizing incidents.

Prioritizing the handling of individual incidents is a critical decision point in the incident response process. Effective information sharing can help an organization identify situations that are of greater severity and demand immediate attention. Incidents should be prioritized based on the relevant factors, such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity, and availability of the organization's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident).

Organizations should use the lessons learned process to gain value from incidents.

After a major incident has been handled, the organization should hold a lessons learned meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices. Lessons learned meetings can also be held periodically for lesser incidents as time and resources permit. The information accumulated from all lessons learned meetings should be used to identify and correct systemic weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new team members.

- Appendix A contains incident response scenarios and questions for use in incident response tabletop discussions.
- Appendix B provides lists of suggested data fields to collect for each incident.
- Appendices C and D contain a glossary and acronym list, respectively.
- Appendix E identifies resources that may be useful in planning and performing incident response.
- Appendix F covers frequently asked questions about incident response.
- Appendix G lists the major steps to follow when handling a computer security incident-related crisis.
- Appendix H contains a change log listing significant changes since the previous revision.

2. Organizing a Computer Security Incident Response Capability

Organizing an effective computer security incident response capability (CSIRC) involves several major decisions and actions. One of the first considerations should be to create an organization-specific definition of the term “incident” so that the scope of the term is clear. The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done. The plan, policies, and procedures should reflect the team’s interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations. This section provides not only guidelines that should be helpful to organizations that are establishing incident response capabilities, but also advice on maintaining and enhancing existing capabilities.

2.1 Events and Incidents

An *event* is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. *Adverse events* are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

A *computer security incident* is a violation or imminent threat of violation¹ of computer security policies, acceptable use policies, or standard security practices. Examples of incidents² are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

2.2 Need for Incident Response

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. The concept of computer security incident response has become widely accepted and implemented. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling

¹ An “imminent threat of violation” refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet.

² For the remainder of this document, the terms “incident” and “computer security incident” are interchangeable.

future incidents and to provide stronger protection for systems and data. An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

Besides the business reasons to establish an incident response capability, Federal departments and agencies must comply with law, regulations, and policy directing a coordinated, effective defense against information security threats. Chief among these are the following:

- OMB's Circular No. A-130, Appendix III,³ released in 2000, which directs Federal agencies to "ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations ... and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance."
- FISMA (from 2002),⁴ which requires agencies to have "procedures for detecting, reporting, and responding to security incidents" and establishes a centralized Federal information security incident center, in part to:
 - "Provide timely technical assistance to operators of agency information systems ... including guidance on detecting and handling information security incidents ...
 - Compile and analyze information about incidents that threaten information security ...
 - Inform operators of agency information systems about current and potential information security threats, and vulnerabilities"
- Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*⁵, March 2006, which specifies minimum security requirements for Federal information and information systems, including incident response. The specific requirements are defined in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*⁶, May 2007, which provides guidance on reporting security incidents that involve PII.

2.3 Incident Response Policy, Plan, and Procedure Creation

This section discusses policies, plans, and procedures related to incident response, with an emphasis on interactions with outside parties.

2.3.1 Policy Elements

Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements:

- Statement of management commitment
- Purpose and objectives of the policy

³ <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

⁴ <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

⁵ <http://csrc.nist.gov/publications/PubsFIPS.html>

⁶ <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>

- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process
- Prioritization or severity ratings of incidents
- Performance measures (as discussed in Section 3.4.2)
- Reporting and contact forms.

2.3.2 Plan Elements

Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

The organization's mission, strategies, and goals for incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan. Section 2.4.1 discusses the types of structures.

Once an organization develops a plan and gains management approval, the organization should implement the plan and review it at least annually to ensure the organization is following the roadmap for maturing the capability and fulfilling their goals for incident response.

2.3.3 Procedure Elements

Procedures should be based on the incident response policy and plan. Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the

priorities of the organization are reflected in response operations. In addition, following standardized responses should minimize errors, particularly those that might be caused by stressful incident handling situations. SOPs should be tested to validate their accuracy and usefulness, then distributed to all team members. Training should be provided for SOP users; the SOP documents can be used as an instructional tool. Suggested SOP elements are presented throughout Section 3.

2.3.4 Sharing Information With Outside Parties

Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever appropriate, such as contacting law enforcement, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other involved parties, such as Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams.

Organizations may also proactively share relevant incident indicator information with peers to improve detection and analysis of incidents. The incident response team should discuss information sharing with the organization's public affairs office, legal department, and management before an incident occurs to establish policies and procedures regarding information sharing. Otherwise, sensitive information regarding incidents may be provided to unauthorized parties, potentially leading to additional disruption and financial loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes.

The following sections provide guidelines on communicating with several types of outside parties, as depicted in Figure 2-1. The double-headed arrows indicate that either party may initiate communications. See Section 4 for additional information on communicating with outside parties, and see Section 2.4 for a discussion of communications involving incident response outsourcers.



Figure 2-1. Communications with Outside Parties

2.3.4.1 The Media

The incident handling team should establish media communications procedures that comply with the organization's policies on media interaction and information disclosure.⁷ For discussing incidents with the media, organizations often find it beneficial to designate a single point of contact (POC) and at least one backup contact. The following actions are recommended for preparing these designated contacts and should also be considered for preparing others who may be communicating with the media:

- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.

⁷ For example, an organization may want members of its public affairs office and legal department to participate in all incident discussions with the media.

The memo.

Envision that this memo will be used to help your client become compliant. The points to address are below.

1. What cybersecurity and data privacy policies and procedures do you consider mandatory in NY State?
2. Is the type of firm a consideration when you determine what cybersecurity and data privacy policies and procedures are mandatory?
 1. Why or why not?
3. What information do you have that supports your policy and procedure selections?
 1. Are your selections based upon best practices, regulations, laws or other authorities?

The paper shall be seven pages, stapled on the top left corner, with each page numbered x of y at the bottom. Double space the memo, use one-inch margins all around and use either times new roman, courier new or an equivalent 11-12 point font.

Please also provide a one-page executive summary.

The core reference materials for the memo will be the NY State Department of Financial Services Cybersecurity Regulation, caselaw and enforcement actions. Additional information used to support your positions can be derived from other sources, such as periodicals, in-person interviews or internet articles.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 10/4/2017

-----X
JESSIE SACKIN, et al.,

Plaintiffs,

-against-

TRANSPERFECT GLOBAL, INC.,

Defendant.

-----X

17 Civ. 1469 (LGS)

OPINION AND ORDER

LORNA G. SCHOFIELD, District Judge:

Plaintiffs filed this purported class action against TransPerfect Global, Inc. (“TransPerfect” or “Defendant”) on February 27, 2017, stemming from a data breach of TransPerfect’s computer systems that disclosed Plaintiffs’ sensitive personally identifiable information (“PII”) to hackers. TransPerfect moves to dismiss the Amended Complaint (“Complaint”) pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). As discussed below, the Rule 12(b)(1) motion is denied because Plaintiff has standing to sue. The Rule 12(b)(6) motion is granted in part, dismissing only the claim of breach of express contract.

I. BACKGROUND

The following facts are drawn from the Complaint and accepted as true for the purpose of this motion. Defendant employs over 4,000 individuals. The company maintains a corporate privacy policy and security manual that describes “robust procedures designed to protect the PII with which it is entrusted.” However, unlike other similarly situated companies, TransPerfect did not train employees on data security; did not erect digital firewalls and did not maintain PII retention and destruction protocols.

Defendant understood the prevalence of cyber-attacks on corporate records and

appreciated the gravity of the risk posed by such attacks. High-profile corporate data breaches dominated recent headlines, and 282 breaches were publicly reported between 2014 and 2015. Defendant's own website warns clients that cyber-attacks "are neither new nor infrequent." The website cautions, "never send your credit card number, Social Security number, bank account number, driver's license number or similar details in an email," because email "is generally not secure" and is the method of communication "most vulnerable to hacking."

On or about January 17, 2017, at least one TransPerfect employee received a "phishing" email. The email appeared to come from TransPerfect's CEO, but actually was sent by unidentified cyber-criminals. The email asked for the W-2 forms and payroll information of all current and former TransPerfect employees. Because TransPerfect's cyber-security was not up to industry par, at least one TransPerfect employee sent the information to the hackers in an unencrypted format. As a result, cyber-criminals obtained Plaintiffs' names, addresses, dates of birth, Social Security numbers, direct deposit bank account numbers and routing numbers.

Hackers can use PII to obtain by fraud employment, loans, credit cards and can file tax returns. Criminals can also use PII to steal government benefits and create false identification for use in further schemes. Stolen PII is frequently bought and sold amongst various criminals on "dark markets." TransPerfect responded to the breach by offering Plaintiffs two free years of enrollment in an identity theft *monitoring* service. Plaintiffs purchased *preventive* services.

II. LEGAL STANDARDS

"A district court properly dismisses an action under Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction if the court lacks the statutory or constitutional power to adjudicate it, such as when . . . the plaintiff lacks constitutional standing to bring the action." *Cortlandt St. Recovery Corp. v. Hellas Telecomms., S.A.R.L.*, 790 F.3d 411, 416–17 (2d Cir. 2015) (internal

citation omitted). The task of the district court is to determine whether the “[p]leading allege[s] facts that affirmatively and plausibly suggest that [the plaintiff] has standing to sue.” *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016) (internal quotation marks omitted). “In resolving a motion to dismiss under Rule 12(b)(1), the district court must take all uncontroverted facts in the complaint . . . as true, and draw all reasonable inferences in favor of the party asserting jurisdiction.” *Fountain v. Karim*, 838 F.3d 129, 134 (2d Cir. 2016) (quoting *Tandon v. Captain’s Cove Marina of Bridgeport, Inc.*, 752 F.3d 239, 243 (2d Cir. 2014)). “The plaintiff bears the burden of alleging facts that affirmatively and plausibly suggest that it has standing to sue.” *Cortland*, 790 F.3d at 417 (internal quotation marks omitted). The issue of subject matter jurisdiction is resolved before turning to the sufficiency of the Complaint. *See generally Carver v. Nassau Cty. Interim Fin. Auth.*, 730 F.3d 150, 156 (2d Cir. 2013) (“Normally, in cases involving the issue of Article III subject matter jurisdiction, this issue would have to be addressed first.”).

To survive a motion to dismiss under Rule 12(b)(6), “a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* On a Rule 12(b)(6) motion, “all factual allegations in the complaint are accepted as true and all inferences are drawn in the plaintiff’s favor.” *Littlejohn v. City of N.Y.*, 795 F.3d 297, 306 (2d Cir. 2015).

III. DISCUSSION

A. Subject Matter Jurisdiction

The motion to dismiss for lack of subject matter jurisdiction is denied because the

Complaint “affirmatively and plausibly” alleges facts sufficient to establish standing. *See HealthPort Techs.*, 822 F.3d at 56. The Complaint alleges four injuries as a consequence of the data breach: (1) an imminent risk of future identity theft; (2) lost time and money expended to mitigate the threat of identity theft; (3) diminished value of personal information; and (4) a loss of privacy. Because the first and second alleged harms satisfy constitutional standing requirements, this opinion does not address the other two claimed injuries.

“[T]he irreducible constitutional minimum of standing contains three elements.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). “The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v Robins*, 136 S. Ct. 1540, 1547 (2016) (internal quotation marks and citation omitted). Defendant challenges only the first element, arguing that the Complaint does not plead injury in fact. As explained below, this argument is incorrect.

To satisfy the injury-in-fact requirement, a plaintiff must allege “an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *John v. Whole Foods Mkt. Grp.*, 858 F.3d 732, 736 (2d Cir. 2017) (citing *Spokeo*, 136 S. Ct. at 1548). Allegations of future harm establish injury in fact as long as the future harm is “certainly impending.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013). By contrast, mere “[a]llegations of possible future injury are not sufficient.” *Id.* (internal quotation marks omitted). While “imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes” *Id.*

The harms alleged in the Complaint do not stretch imminence beyond its breaking point. The allegations that Defendant has provided Plaintiffs' names, addresses, dates of birth, Social Security numbers and bank account information directly to cyber-criminals creates a risk of identity theft sufficiently acute so as to fall comfortably into the category of "certainly impending." The most likely and obvious motivation for the hacking is to use Plaintiffs' PII nefariously or sell it to someone who would. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."). Circuit courts addressing this issue consistently have held that Article III does not require Plaintiffs to wait for their identities to be stolen before seeking legal recourse. *See Attias v. Carefirst, Inc.*, 865 F.3d 620, at 629–30 (D.C. Cir. 2017) (holding that alleged increased risk of identity theft was sufficiently imminent to establish standing after a retailer's data breach); *Remijas*, 794 F.3d at 695 (same); *Galaria v. Nationwide Mut. Ins.*, 663 F. App'x 384, 388 (6th Cir. Sept. 12, 2016) (same); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164 (1st Cir. 2011) (same).

While the Second Circuit has yet to address the question, two recent unreported decisions suggest that it will follow the lead of its sister circuits. *See Katz v. Donna Karan Co.*, --- F.3d ---, 2017 WL 4126942, at *5 (2d Cir. Sept. 19, 2017); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. May 2, 2017) (summary order). In *Whalen*, the Second Circuit concluded that the complaint failed to allege standing because the plaintiff never paid a fraudulent charge, nor did she face a plausible threat of future harm. Her "stolen credit card was promptly canceled after the breach and no other personally identifying information -- such as her birth date or Social Security number -- is alleged to have been stolen." *Id.* Similarly, in *Katz*, the Second Circuit

held that a “district court did not clearly err in finding that the bare procedural violation in question [i.e., printing the last six digits of a customer’s credit card number on their store receipt] did not raise a material risk of harm of identity theft.” 2017 WL 4126942, at *6.

Whether the risk of identity theft is sufficiently material to create an injury in fact is “a question for lower courts to determine in the first instance, on a case- and fact-specific basis.” *Id.* Here, a case-specific analysis dictates that standing exists. The Complaint alleges that Defendant divulged information -- including birth dates and social security numbers -- far more sensitive than all or a portion of a credit card number, and that the PII here was provided directly to cybercriminals, and not merely printed on a store receipt.

When a future harm is sufficiently imminent to support standing, a plaintiff’s expenses in taking reasonable measures to prevent the harm’s fruition also may be viewed as an injury in fact. *See Hedges v. Obama*, 724 F.3d 170, 196 (2d Cir. 2013) (the Supreme Court has “sometimes found standing to sue where plaintiffs showed only a substantial risk that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm”) (quoting *Clapper*, 568 U.S. 398, 414 n.5 (2013)); *Nationwide Mut. Ins.*, 663 F. App’x at 388 (stating that, “Plaintiffs’ allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage”). Here, the Complaint alleges that Plaintiffs reasonably incurred the cost identity theft prevention services. Accordingly, the Complaint sufficiently alleges injury in fact, both regarding the risk of identity theft and remedial measures.

In an effort to circumvent the appellate decisions cited above, Defendant cites a handful of distinguishable cases in which courts found standing to be lacking when a plaintiff’s PII was on a stolen computer, and the plaintiffs did not allege or could not show that obtaining their PII

was the motivation for the theft. *See, e.g., Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (stating that “plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information”). Similarly inapt are cases where the stolen PII was significantly less sensitive -- and less useful to thieves -- than the Social Security numbers and banking information taken here. *See, e.g., Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857, 862 (S.D. Ind. 2016) (no standing existed where “[o]nly names, credit card numbers, and card expiration dates were stolen . . .”).

As the allegations of the risk of identity theft and related mitigating expenses are sufficient to allege injury in fact and thereby confer standing, the Court has subject matter jurisdiction. The motion to dismiss based on Rule 12(b)(1) is denied.

B. Failure to State a Claim

The Complaint pleads five causes of action: (1) common law and statutory negligence; (2) breach of express contract; (3) breach of implied contract; (4) unjust enrichment and (5) violations of N.Y. Labor Law 203-d.¹ Defendant’s motion to dismiss the express contract claim is granted, but its motion to dismiss the other claims is denied.

1. Negligence

“Under New York law, in order to recover on a claim for negligence, a plaintiff must show (1) the existence of a duty on defendant’s part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof.” *Caronia v. Philip Morris USA, Inc.*, 715 F.3d 417,

¹ New York law applies as the parties assume that it does. “The parties’ briefs assume that [New York] state law governs this case, and ‘such implied consent is ... sufficient to establish the applicable choice of law.’” *Trikona Advisers Ltd. v. Chugh*, 846 F.3d 22, 31 (2d Cir. 2017) (quoting *Arch Ins. Co. v. Precision Stone, Inc.*, 584 F.3d 33, 39 (2d Cir. 2009)).

428 (2d Cir. 2013) (internal quotation marks omitted). The Complaint sufficiently alleges that TransPerfect breached a duty owed to Plaintiffs under both common law and negligence per se principles, and that Plaintiffs suffered injury as a result.

a) Breach of Common law Duty

The Complaint alleges a cognizable legal duty -- that Defendants had a duty to safeguard Plaintiffs' and class members' PII. "The definition and scope of an alleged tortfeasor's duty owed to a plaintiff is a question of law." *Pasternack v Lab. Corp. of Am. Holdings*, 59 N.E.3d 485, 490 (N.Y. 2016). In making that determination, "the court must settle upon the most reasonable allocation of risks, burdens and costs among the parties and within society, accounting for the economic impact of a duty, pertinent scientific information, the relationship between the parties, the identity of the person or entity best positioned to avoid the harm in question, the public policy served by the presence or absence of a duty and the logical basis of a duty" *In re N.Y. City Asbestos Litig.*, 59 N.E.3d 458, *8 (N.Y. 2016). "Foreseeability defines the scope of a duty once it has been recognized." *Id.* at *9.

Applying these factors, employers have a duty to take reasonable precautions to protect the PII that they require from employees. Employees ordinarily have no means to protect that information in the hands of the employer, nor is withholding their PII a realistic option. The employer is "best positioned to avoid the harm in question" *Id.* at *8. *See also Katz v. United Synagogue of Conservative Judaism*, 23 N.Y.S.3d 183, 184 (1st Dep't 2016) ("The parties' relationship may create a duty where it 'places the defendant in the best position to protect against the risk of harm and the specter of limitless liability is not present.'"). Employees -- much more than employers -- suffer the harmful consequences of a data breach of the employer. Potential liability in the absence of reasonable care provides employers with an

economic incentive to act reasonably in protecting employee PII from the threat of cyberattack.

The Complaint also sufficiently alleges that TransPerfect violated its duty to take reasonable steps to protect its employees' PII. The Complaint alleges that TransPerfect was aware of the sensitivity of PII and the need to protect it; TransPerfect's website warns, "never send . . . credit card number[s], Social Security number[s], bank account number[s] . . . or similar details in an email," because email "is generally not secure" and is "vulnerable to hacking." The Complaint also alleges that, despite this knowledge, Defendant failed to take reasonable steps to prevent the wrongful dissemination of Plaintiffs' PII -- including erecting a digital firewall, conducting data security training and adopting retention and destruction policies -- such that a TransPerfect employee responded to a phishing email by sending Plaintiffs' PII to cyber-criminals. These allegations are sufficient to state a claim for negligence.

b) Breach of Statutory Duty

The Complaint sufficiently alleges negligence *per se*. "Under the rule of negligence *per se*, if (1) a statute is designed to protect a class of persons, (2) in which the plaintiff is included, (3) from the type of harm which in fact occurred as a result of its violation, the issues of the defendant's duty of care to the plaintiff and the defendant's breach of that duty are conclusively established upon proof that the statute was violated." *German by German v. Fed. Home Loan Mortg. Corp.*, 896 F. Supp. 1385, 1396 (S.D.N.Y. 1995) (numbering added) (citing *Martin v. Herzog*, 126 N.E. 814 (N.Y. 1920)); PROSSER AND KEETON ON THE LAW OF TORTS, at 229–30 (5th ed. 1984); *accord Jordan v. Tucker, Albin & Assocs.*, No. 13 civ. 6863, 2017 WL 2223918, at *12 (E.D.N.Y. May 19, 2017).

The Complaint sufficiently alleges breach of a statutory duty. First, New York Labor Law makes it illegal for an employer to "communicate an employee's personal identifying

information to the general public.” N.Y. LAB. LAW § 203-d(1)(d) (McKinney 2009). The statute defines “personal identifying information” to include: the employee’s “social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent’s surname prior to marriage, or drivers’ license number.” *Id.* § 203-d(1)(c). Second, Plaintiffs are within the class of persons -- employees -- the law is designed to protect. Third, exposure of PII is precisely the harm that the statute seeks to prevent. Even the alleged method of Defendant’s breach is contemplated by the statute, which states, “It shall be presumptive evidence that a violation . . . was knowing if the employer has not put in place policies or procedures to safeguard against” the disclosure of PII. *Id.* § 203-d(3).

c) Injury

Defendant’s 12(b)(6) motion is somewhat duplicative of its 12(b)(1) motion, because both rely heavily on a claimed lack of injury. Defendant argues that the negligence claim is deficient because “Plaintiff does not properly plead that he suffered any actual cognizable injury.” This argument is unpersuasive; the Complaint sufficiently alleges injuries stemming from Defendant’s breach of duty.

As discussed above, the Complaint adequately alleges that Plaintiffs face an imminent threat of identity theft and have purchased preventive services to mitigate the threat. These mitigation expenses satisfy the injury requirements of negligence; otherwise Plaintiffs would face an untenable Catch-22. Under New York’s “doctrine of avoidable consequences,” a plaintiff must “minimize damages” caused by a defendant’s tortious conduct, and can recover mitigation costs for any “action [] reasonable under the circumstances” *Revelations Perfume & Cosmetics, Inc. v. Nelson*, No. 603350/2008, 2012 WL 1434856, at *3 (N.Y. Sup. Ct. Apr. 12, 2012) (citing *Fed. Ins. Co v. Sabine Towing & Transp. Co.*, 783 F.2d 347, 350–51 (2d

Cir.1986)). Accordingly, Plaintiffs were required to take reasonable steps to mitigate the consequences of the data breach; they could not passively wait for their identities and money to be stolen. The Complaint sufficiently alleges that Plaintiffs have taken such reasonable steps, and that they are entitled to reimbursement.

The economic loss rule -- which in the “absence of any personal injury or property damage precludes plaintiffs' claims for economic injury” in negligence cases -- does not bar Plaintiffs’ negligence claim, as Defendant suggests, for two reasons. *532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc.*, 750 N.E.2d 1097, 1101 (N.Y. 2001). First, the rule is inapplicable because the Complaint does not allege a products liability claim. *See Id.* at 1101 n.1 (stating that the economic loss rule “stands for the proposition that an end-purchaser of a product is limited to contract remedies and may not seek damages in tort for economic loss against a manufacturer”); *Travelers Cas. & Sur. Co. v. Dormitory Auth.-State N.Y.*, 734 F. Supp. 2d 368, 378 (S.D.N.Y. 2010). Second, despite the economic loss rule, “[a] negligence claim may be brought provided that the plaintiff alleges that ‘a legal duty independent of the contract itself has been violated.’” *Emerald Town Car of Pearl River, LLC v. Phila. Indem. Ins. Co.*, No. 16 Civ. 1099, 2017 WL 1383773, at *4 (S.D.N.Y. Apr. 12, 2017) (citing *Dorking Genetics v. United States*, 76 F.3d 1261, 1269 (2d Cir. 1996)). Also, as detailed above, the Complaint alleges breach of common law and statutory duties distinct from Defendant’s contractual duties. TransPerfect’s motion to dismiss Plaintiffs’ negligence claim is denied.

2. Breach of Contract

“Under New York law, a breach of contract claim requires (1) the existence of an agreement, (2) adequate performance of the contract by the plaintiff, (3) breach of contract by the defendant, and (4) damages.” *Balk v. N.Y. Inst. of Tech.*, 683 F. App’x 89, 95 (2d Cir. Mar.

23, 2017) (summary opinion) (internal quotation marks omitted). The Complaint pleads breach of express and implied contract as separate causes of action. As detailed below, the express contract claim is dismissed, but the implied contract claim survives.

a) Breach of Express Contract

The Complaint fails to allege a sufficient claim for breach of express contract. It alleges that Plaintiffs' employment contracts "involved a mutual exchange of consideration whereby TransPerfect entrusted Plaintiffs and Class Members with particular job duties and responsibilities in furtherance of TransPerfect's services, in exchange for the promise of employment, with salary, benefits and secure PII."

The Complaint fails to allege any facts to support the conclusion that Defendant expressly contracted to protect employees' PII. The Complaint does not describe any express agreement to that effect, nor does the Complaint attach or quote any contract. In adjudicating express contract claims, "[a] court cannot supply a specific obligation the parties themselves did not spell out." *Wallert v. Atlan*, 141 F. Supp. 3d 258, 286 (S.D.N.Y. 2015) (internal quotation marks omitted). "The plaintiff must identify what provisions of the contract were breached as a result of the acts at issue." *Glob. Packaging Servs., LLC v. Glob. Printing & Packaging*, --- F.Supp.3d ----, 2017 WL 1232731, at *3 (S.D.N.Y. Mar. 31, 2017) (internal quotation marks omitted).

By failing to allege any facts upon which a finding of express contract regarding PII could be predicated, the Complaint engages in the type of "[t]hreadbare recital[] of the elements of a cause of action" that *Iqbal* warned against. 556 U.S. at 678. The second cause of action, for breach of express contract, is dismissed.

b) Breach of Implied Contract

The Complaint states a claim for breach of implied contract. “Under New York law, a contract implied in fact may result as an inference from the facts and circumstances of the case, though not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct.” *Leibowitz v. Cornell Univ.*, 584 F.3d 487, 506–07 (2d Cir. 2009); (internal quotation marks and alterations omitted); *accord Jasper & Black v. Carolina Pad Co.*, No. 10 Civ. 3562, 2012 WL 413869, at *7 (S.D.N.Y. 2012). An implied contract, like an express contract, requires “consideration, mutual assent, legal capacity and legal subject matter.” *Id.* at 507.

Plaintiffs allege conduct and a course of dealing that raise a strong inference of implied contract. TransPerfect required and obtained the PII as part of the employment relationship, evincing an implicit promise by TransPerfect to act reasonably to keep its employees’ PII safe. TransPerfect’s privacy policies and security practices manual -- which states that the company “maintains robust procedures designed to carefully protect the PII with which it [is] entrusted” -- further supports a finding of an implicit promise. *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015) (motion to dismiss contract claims denied based on allegation that “[d]efendants, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard his PII in exchange for his employment”). *Cf. Gone v. Wackenhut Servs. Inc.*, No. 10 Civ. 2495, 2010 WL 2077210, at *2 (S.D.N.Y. May 17, 2010) (noting that limitations on an employer’s power to fire “can be found in the employment contract itself or in other employment-related documents, such as a personnel manual or employee handbook”). While TransPerfect may not have explicitly promised to protect PII from hackers in Plaintiffs’ employment contracts, “it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal

information would not imply the recipient's assent to protect the information sufficiently."

Castillo v. Seagate Tech., LLC, No. 16 civ. 1958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016). The motion to dismiss the breach of implied contract claim is denied.

c) Damages

Defendant reframes the no-injury argument asserting the failure to plead "actual damages arising from the purported breach." The argument is unpersuasive in this context as well. As discussed above, the Complaint adequately pleads a "certainly impending" injury, as well as preventive economic injury. Similar to the tort context, the complaint alleges that Plaintiffs acted "consistent with the general contract principle[] that . . . the injured party has a duty to mitigate." *White v. Farrell*, 987 N.E.2d 244, 252 (N.Y. 2013) (internal quotation marks omitted). Plaintiffs were not legally permitted to watch passively as their identities were stolen and bank accounts drained. Consequentially, the Complaint adequately pleads all the necessary elements of breach of contract.

3. Unjust Enrichment

The claim of unjust enrichment is sufficiently pleaded. "[I]n order to adequately plead such a claim, the plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." *Ga. Malone & Co. v. Rieder*, 973 N.E.2d 743 (N.Y. 2012) (internal quotation marks omitted). The Complaint adequately alleges all three elements -- first, that TransPerfect received the benefits of Plaintiffs' labor; second, that TransPerfect was enriched at Plaintiffs' expense when it chose to cut costs by not implementing security measures to protect Plaintiffs' PII which Defendant required or obtained in the course of Plaintiffs' employment; and third, that it would be inequitable and unconscionable to allow TransPerfect to

retain the money it saved by shirking data-security, while leaving Plaintiffs to suffer the consequences.

The unjust enrichment claim is not precluded by the contract claim. New York law “precludes unjust enrichment claims whenever there is a valid and enforceable contract governing a particular subject matter, whether that contract is written, oral, or implied-in-fact.” *Green Tree Servicing, LLC v. Christodoulakis*, 689 F. App’x 66, 71 (2d Cir. Apr. 28, 2017) (summary order). Only “where a bona fide dispute exists as to the existence of the contract, the plaintiff may proceed on both breach of contract and quasi-contract theories.” *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc.*, 448 F.3d 573, 587 (2d Cir. 2006) (quoting *Nakamura v. Fujii*, 677 N.Y.S.2d 113, 116 (1st Dep’t 1998)). Here, although the Complaint adequately pleads an implied-in-fact contract, Defendant’s opposition suggests that it will dispute that Defendant agreed to be bound in an implied contract with Plaintiffs. *Accord Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 770 (W.D.N.Y. 2017) (declining to dismiss unjust enrichment claim where “the parties dispute whether the parties have an enforceable contract with definite and material terms regarding the provision of data security”). See generally N.Y. Pattern Jury Instr.--Civil 4:1 (“Contracts implied in fact must be distinguished from contracts implied-in-law (quasi contracts), which are not contracts at all but obligations imposed by law through the legal fiction of a contract.”).

4. N.Y. Labor Law § 203-d

Plaintiffs assert that N.Y. Labor Law § 203-d not only provides a basis for negligence per se, but also affords them a private right of action. The text of the statute is silent on private causes of action; however, that silence does not settle the issue. “In the absence of an express private right of action, plaintiffs can seek civil relief in a plenary action based on a violation of

the statute only if a legislative intent to create such a right of action is fairly implied in the statutory provisions and their legislative history.” *Nat’l Convention Servs., L.L.C. v. Applied Underwriters Captive Risk Assurance Co*, 239 F. Supp. 3d 761, 778 (S.D.N.Y. 2017) (internal quotation marks omitted). Courts decide whether a statute fairly implies a private cause of action by analyzing three factors, “of which the third is the most important: (1) whether the plaintiff is one of the class for whose particular benefit the statute was enacted; (2) whether recognition of a private right of action would promote the legislative purpose; and (3) whether creation of such a right would be consistent with the legislative scheme.” *Id.*

All three factors demonstrate that N.Y. Labor Law § 203-d implies a private right of action. First, Plaintiffs are within the class the statute is designed to protect: employees who suffered the precise type of harm that the statute is designed to prevent. Second, an implied right of action is consistent with § 203-d’s legislative purpose. In general, New York Labor Law reflects “a strong legislative policy aimed at redressing the power imbalance between employer and employee.” *Chu Chung v. New Silver Palace Rest.*, 272 F. Supp. 2d 314, 317 (S.D.N.Y. 2003) (internal quotation marks omitted). As § 203-d’s sponsor explained, the specific provision provides “important confidentiality safeguards for employees.” N.Y. Bill Jacket, 2008 S.B. 8376, Ch. 279.

Third, an implied cause of action is consistent with the legislative scheme. Section 203-d provides for administrative enforcement: the “commissioner may impose a civil penalty of up to five hundred dollars on any employer for any knowing violation” An implied private right of action is appropriate to imply in addition to administrative enforcement where “the determination of a violation and the calculation of resulting damages do not require any special agency expertise.” *Maimonides Med. Ctr. v. First United Am. Life Ins.*, 981 N.Y.S.2d 739, 748

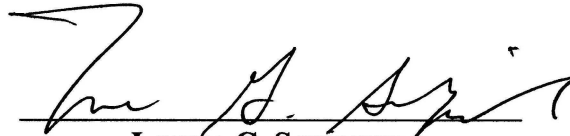
(2d. Dep’t 2014). Implied private causes of action are also especially appropriate in situations where the statute uses mandatory “shall” language.” *Id.* Here, no special agency expertise is required to determine if PII was wrongly disclosed, and the statute demands that employers “*shall* not . . . communicate an employee’s personal identifying information” N.Y. LAB. LAW § 203-d (McKinney 2009) (emphasis added). Accordingly, § 203-d implies a private right of action.

IV. CONCLUSION

For the foregoing reasons, TransPerfect’s motion to dismiss for lack of subject matter jurisdiction is DENIED. TransPerfect’s motion to dismiss for failure to state a claim is GRANTED with respect to Plaintiffs’ express contract cause of action, and otherwise DENIED. The Clerk of Court is respectfully directed to close Dkt. #20. Defendant’s request for oral argument (Dkt. 29) is DENIED as moot.

SO ORDERED.

Dated: October 4, 2017
New York, New York



LORNA G. SCHOFIELD
UNITED STATES DISTRICT JUDGE