PAUL HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

April 2015

Caught in the Crossfire: The Rising Threat of Cyberattacks on Financial Institutions and the Heightened Expectations of Financial Regulators

BY THE GLOBAL BANKING AND PAYMENT SYSTEMS PRACTICE

Within the last year, cyberattacks involving data breaches caused by hackers or unauthorized parties have grown in number and sophistication. While cyberattacks pose a threat to all organizations, financial institutions are particularly at risk, as they hold not only funds but also private data on consumers and commercial entities. In recent years, cyber criminals have used online banking and payment systems to transfer money directly from financial institutions' accounts to their own accounts, and have even seized control of bank ATMs and caused cash to be dispensed at predetermined times to waiting recipients in complex and orchestrated cyber heists. The Moscow-based security firm Kaspersky Lab estimates that one coordinated cyberattack against banks and financial institutions initiated in late 2013 may have caused losses of up to USD$1 billion,[1] and that number may be higher. According to the Identity Theft Resource Center, given the number of data breaches that often go unreported. Perhaps more compelling than the cost of lost funds is the organizational cost to an institution after a data breach, including related remediation and regulatory compliance costs.

…reported data breaches in the U.S. hit a record high of 783 incidents in 2014; however, that number is likely much higher…

Given the real and rising threat of cyberattacks against financial institutions and the potential for significant impact to the global economy, financial regulators and law enforcement are becoming increasingly alert to such risks and heightening their scrutiny of cybersecurity programs. In the wake of heightened regulatory expectations, financial institutions may find themselves fighting a two-front war—preventing cybercriminals from gaining access to funds and private data, and satisfying the compliance requirements and requests of their regulators and law enforcement. In combatting cybercrime and cyberterrorism, financial institutions are finding it more important than ever to work with their regulators and law enforcement, while recognizing that the institutions' goals and the goals of regulatory and law enforcement authorities may not always neatly align.

The Rising Threat of Cyberattacks

Cyberattacks generally take two forms—untargeted and targeted attacks. In an untargeted attack, criminals do not focus on a particular victim but target as many devices, users or services as possible through cyberattacks such as phishing (sending mass emails requesting sensitive information or directing users to visit fake websites), water holing (creating fake websites or compromising legitimate

websites in order to exploit visitors), ransomware (locking out and holding files hostage via encryption or other means until the owner of the system pays a ransom to have the files unlocked, which often does not happen even after the ransom is paid), and scanning (attacking wide sections of the internet randomly).[2] Not surprisingly, targeted attacks pose a greater threat to financial institutions—in a targeted attack the criminals specifically tailor the attack to the financial institution, including through spear phishing (sending emails with malicious software attached to individuals at the institution), launching distributed denial of service attacks (shutting off internet access to bank services by directing waves of internet traffic from compromised computers to the bank, sometimes involving efforts to distract bank personnel while criminals gain unauthorized remote access to accounts),[3] and subverting the supply chain (attacking the equipment or software that is delivered to the organization).[4] Cyber terrorists are increasingly employing targeted attack strategies.

Cyberattacks—Increasingly Sophisticated Strategies

In the series of coordinated bank cyberattacks that was initiated in late 2013, an unknown group of criminals has already stolen as much as USD$1 billion from banks and financial institutions,[5] and the attacks apparently are still active.[6] The criminal group gained access to 100+ banking entities via spear phishing emails sent to bank employees. The emails appeared to be legitimate banking communications in the form of Microsoft Word and CPL files, indicating the criminals' sophisticated knowledge of the industry.[7] The emailed files contained malware that, once the files were opened onto the institution's network system, exploited vulnerabilities in Microsoft Office and Microsoft Word and executed a remote backdoor providing criminals remote access to the banks' computers. Once access was achieved, the attackers installed additional software and spied on the activities of bank employees and administrators through video surveillance, allowing the criminals to impersonate legitimate users to perform later actions, including manipulating accounts, transferring money and ordering ATMs to dispense cash at designated times and places.[8] In most cases, the institutions' accounts were compromised for several months before the attackers actually stole any funds.[9] Particularly concerning to banks is that, according to Kaspersky Lab's Principal Security Researcher, the "bank heists were surprising because it made no difference to the criminals what software the banks were using."[10]

...financial institutions may find themselves fighting a two-front war—preventing cybercriminals from gaining access to funds and private data, and satisfying the compliance requirements and requests of their regulators and law enforcement.

This is just one example of the wave of recent cyberattacks targeting banks and other financial institutions, and it indicates a clear trend toward more sophisticated attacks by cybercriminals familiar with the financial industry. Understandably, the increase in the number and sophistication of cyberattacks has alarmed financial regulators and law enforcement officials. The White House and Congress have also taken notice.

Recent Attacks on Financial Institutions

In 2014, cybercriminals waged what appears to be an expanding offensive of cyberattacks on financial institutions. Among the more notable cyberattacks was a July 2014 attack involving a large regional bank network that was accessed by an unknown third party, and placed over 72,000 customer accounts at risk of exposure. Following an investigation, it was determined that the unauthorized third party may have obtained access to customer information, including names, addresses, account numbers, account balances, and personal identification numbers.[11] In another cyberattack several weeks later, a large national bank was victimized by one of the largest cybersecurity breaches involving a U.S. bank, with approximately 76 million household and 7 million small business accounts

compromised. The cyberattackers gained access to the bank's servers that housed consumer account information. Due to the manner in which the cyberattack was orchestrated, the attack went undetected for almost two months before the bank discovered it and moved to close access paths of over 90 servers. The bank worked closely with law enforcement and banking regulators to determine the scope and method of the attack, and ensure that issues with network system vulnerabilities were addressed.[12]

A particular aspect of cyberattacks that complicates the ability of banks effectively to monitor and maintain adequate cybersecurity protocols is that sometimes an attack may come from very conventional means that exploit a network system or process vulnerability that may not be evident or obvious to an institution. This was the case when a highly publicized mobile payment platform was unveiled and cybercriminals seized upon a method employing identity theft, rather than hack into the payment system, to exploit the customer sign-up process to validate credit cards for use on the new payment system.[13] The cyber criminals exploited the sign-up process at the front end by taking easily obtainable customer information to validate a credit card to participate in the mobile payment system counting on the fact that some banks would be motivated to streamline the customer account sign-up process and not require additional verification information to validate customer credentials, i.e., to make the process as seamless as possible. As a result, notwithstanding an extremely secure token security methodology embedded in the mobile payment platform, cybercriminals were able to infiltrate customer bank accounts at the bank end of the validation process via relatively rudimentary means. As a result, the mobile payment provider and banks are reviewing procedures to prevent this issue from repeating, including the possibility of utilizing a PIN issued by a bank to its customer for a one-time use to register a new card.[14]

...sometimes an attack may come from very conventional means that exploit a network system or process vulnerability that may not be evident or obvious to an institution.

Policymakers, Regulators and Law Enforcement on High Alert

The federal government has recognized and taken various steps to respond to the growing threat of cyberterrorism, including two recent Executive Orders ("EOs") from the White House and legislative efforts from Capitol Hill. On February 13, 2015, President Obama signed EO 13691, "Promoting Private Sector Cybersecurity Information Sharing."[15] The Order encourages the sharing of cybersecurity threat information within the private sector and between the private sector and the government through the formation of information sharing and analysis organizations ("ISAOs"). EO 13691 also directs the Department of Homeland Security ("DHS") to develop a common set of voluntary standards for ISAOs.

On April 1, 2015, the President signed another Executive Order, EO 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities."[16] The Order, among other things, declares the increase in foreign originated malicious cyber activity a national emergency, and authorizes the imposition of sanctions on any individuals or entities determined to be responsible for, or complicit in, cyber-related activities that "are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health or financial stability of the United States."[17] Pursuant to EO 13694, the Treasury Secretary, in consultation with the U.S. Attorney General and Secretary of State, has authority to promulgate rules or redelegate its rulemaking authority to other federal agencies. Although the Order does not expressly impose new duties on financial institutions—other than a prohibition from engaging in transactions with sanctioned

persons and entities—the eventual rules could increase the cybersecurity compliance burdens on financial institutions.

Policymakers on Capitol Hill have also been busy addressing concerns from cybersecurity risks. Lawmakers have been grappling with cybersecurity legislation since 2012, when the Senate twice failed to pass a bill due to business concerns that new legislation would put too heavy a burden on the private sector. This year, however, these concerns may give way to greater concerns of national security. On April 22, 2015, the U.S. House of Representatives passed H.R. 1560, the Protecting Cyber Networks Act,[18] which would enable private companies to share cyber threat indicators with each other and, on a purely voluntary basis, with the federal government. Generally, H.R. 1560 includes strong protections for individual privacy and civil liberties, including restricting the sharing of information with the National Security Agency and the U.S. Department of Defense. On April 23, 2015, the House passed a complementary measure to H.R. 1560, the National Cybersecurity Protection Advancement Act, H.R. 1731,[19] which would also provide liability protections for companies that share cyber-threat information with the DHS National Cybersecurity and Communications Integration Center ("NCCIC") any indicators or defensive measures obtained from their own information systems, or the information systems of other federal or non-federal entities. H.R. 1731 would also establish a private cause of action against a federal agency that intentionally or willfully violates restrictions on the use and protection of voluntarily shared indicators or defensive measures. Both House bills have been sent to the Senate for its consideration.

This year, the FBI and the U.K.'s MI5 plan to stage war game cyberattacks to test the City of London and Wall Street's cybersecurity infrastructure and response capabilities…

In addition to these policy initiatives, U.S. and U.K. law enforcement agencies are jointly preparing to develop their defenses against cyberattacks. This year, the U.S. Federal Bureau of Investigation ("FBI") and the U.K.'s MI5 plan to stage war game cyberattacks to test the City of London and Wall Street's cybersecurity infrastructure and response capabilities as both countries' financial institutions and law enforcement work to enhance defenses against cyberterrorism.[20] In addition, DHS has an extensive cybersecurity mandate and has established the NCCIC as a "24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement."[21]

State and federal bank regulators are also at full alert. As Benjamin Lawsky, head of New York's Department of Financial Services ("NYDFS"), has observed, a large enough cyberattack on Wall Street firms could "spill over into the broader economy." As noted by Lawsky, regulators "are concerned that within the next decade, or perhaps sooner, we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time."[22] As a result, NYDFS is considering new anti-money laundering rules, including requiring bank executives to certify the quality of their money transaction monitoring and imposing random NYDFS audits on licensed banks to assess their systems for flagging suspicious transactions.[23]

…regulators "are concerned that within the next decade, or perhaps sooner, we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time." Benjamin Lawsky, NYDFS

Finally, as most banks know by now, the federal banking agencies ("FBAs")[24] have been steadily increasing their oversight and supervision of cybersecurity risks for some time. As noted in the Office of the Comptroller of the Currency ("OCC") in the agency's spring 2013 Semiannual Risk Perspective Report, the "increasing volume and sophistication of cyber-threats poses an ongoing challenge

to the confidentiality, integrity, and availability of systems. . . .Criminals seeking to steal information, commit fraud, or disrupt, degrade, or deny access to information systems strain bank resources and can cause financial, operational, and reputational harm."[25] Two years later, the FBA's cybersecurity concerns are even more pronounced. As noted by Sarah J. Dahlgren of the Federal Reserve Bank of New York, "cybersecurity is a 'new normal.' It is going to become part of our vocabulary in nearly every exam we conduct, conversation we have with senior management, and conversation about the future of financial services."[26] To date, FBA efforts include issuing cybersecurity and data breach guidance through the Federal Financial Institutions Examination Council ("FFIEC") in response to the rising threat of cyberterrorism, as discussed in greater detail below.

Heightened Regulatory Expectations

In connection with the FBA's increasing concerns regarding cyberattacks, over the past few years the FBAs have issued various cybersecurity and data breach guidance. In 2014, the FFIEC piloted a cybersecurity examination work program involving over 500 community institutions "to evaluate their preparedness to mitigate cyber risks."[27] Generally, the FFIEC indicated that "the level of cybersecurity inherent risk varies significantly across financial institutions."[28] In this regard, cybersecurity inherent risk refers to "the amount of risk posed by a financial institution's activities and connections, notwithstanding risk-mitigating controls in place."[29] According to the FFIEC report, an institution's "cybersecurity inherent risk" includes an evaluation of the "connection types, products and services offered" by the institution, as well as the technologies the institution uses for such systems. The FFIEC 2014 cybersecurity assessment concluded that "institutions are critically dependent on [information technology] to conduct business operations," and

…"cybersecurity is a 'new normal.' It is going to become part of our vocabulary in nearly every exam we conduct, conversation we have with senior management, and conversation about the future of financial services." Sarah J. Dahlgren, FRBank of New York

> this dependence, coupled with increasing sector interconnectedness and rapidly evolving cyber threats, reinforces the need for engagement by the board of directors and senior management, including understanding the institution's cybersecurity inherent risk; routinely discussing cybersecurity issues in meetings; monitoring and maintaining sufficient awareness of threats and vulnerabilities; establishing and maintaining a dynamic control environment; managing connections to third parties; and developing and testing business continuity and disaster recovery plans that incorporate cyber incident scenarios.[30]

Based on the findings from the 2014 pilot program, the FFIEC describes cybersecurity preparedness as requiring risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience.[31] Generally, the 2014 assessment report describes these core components of an effective cyber risk management program as follows:

- **Risk management and oversight** involves governance, allocation of resources, and training of employees. The FFIEC recommends that directors and senior management routinely discuss cybersecurity issues to create a security culture at the institution, and that the institution clearly defines the roles and responsibility for identifying, assessing, and managing cybersecurity risks across the institution. Training programs should be updated to respond to changing circumstances and provided routinely.

- **Threat intelligence and collaboration** requires the analysis of information to identify, track and predict cyberattacks, and includes monitoring and sharing information from multiple sources. According to the FFIEC, institutions should participate in information sharing forums, like the Financial Services Information Sharing and Analysis Center ("FS-ISAC"),[32] and identify relevant points of contact with law enforcement and regulators. Additionally, the FFIEC recommends maintaining event logs to understand cyber events after they occur to broaden the institution's understanding of trends and potential vulnerabilities.

- **Cybersecurity controls** should include preventative controls to impede unauthorized access to systems, detective controls to identify attacks, and corrective controls to address identified vulnerabilities. Financial institutions should incorporate measures that impede unauthorized access to their internal systems and consumer data, such as by encrypting consumer information. Institutions should also invest in and implement anti-virus and anti-malware detection tools, routinely scan information technology networks for vulnerabilities and suspicious activity, and test systems for exposure. Furthermore, institutions should develop and test processes for shutting down unauthorized access and remediating damage to IT systems.

- **External dependency management** involves connectivity to third party providers and customers and the financial institutions' oversight of these relationships. The FFIEC recommends that institutions consider the risks of each relationship and evaluate a third party's cybersecurity controls before entering into third party contracts.

- **Cyber incident management and resilience** involves incident detection, response, mitigation and reporting. According to the FFIEC, financial institutions should have procedures for notifying customers, regulators and law enforcement when incidents occur. Institutions should also develop business continuity and disaster recovery plans, and test such plans across business functions to identify gaps before cyberattacks occur.

On March 17, 2015, the FFIEC announced that it plans to develop a cybersecurity self-assessment tool this year to assist institutions in evaluating their cybersecurity risks and risk management capabilities. It is expected that the self-assessment tool will track the core cyber risk management components noted above. The FFIEC also noted that it plans to improve its collaboration with other regulators and law enforcement, and enhance incident analysis, crisis management, training, policy development, and technology service provider strategies. Two weeks later, on March 30, 2015, the FFIEC issued two joint statements—a Joint Statement on Cyberattacks Compromising Credentials[33] and a Joint Statement on Destructive Malware.[34] While the FFIEC agencies suggested the two joint statements were merely repetitive of general guidance already issued, it appears both may signal a new level of regulatory oversight and scrutiny of depository institutions' cyber risks.

FFIEC plans to develop a cybersecurity self-assessment tool this year to assist institutions in evaluating their cybersecurity risks and risk management capabilities.

In the Joint Statement on Cyberattacks Compromising Credentials, the FFIEC agencies recommend fighting the threat of cyberattacks compromising credentials by having banks review their risk management practices and controls related to information technology networks and authentication, authorization, fraud detection, and response management systems and processes. In particular, the Joint Statement recommends some familiar themes, including:

- Conducting ongoing information security risk assessments;
- Performing security monitoring, prevention, and risk mitigation;
- Protecting against unauthorized access;
- Implementing and testing controls around critical systems regularly;
- Enhancing information security awareness and training programs; and
- Participating in industry information-sharing forums.

The companion Joint Statement on Destructive Malware provides that financial institutions and technology service providers serving the financial sector should enhance their information security programs to ensure they are able to identify, mitigate, and respond to a destructive malware attack. The Joint Statement further notes that, in addressing destructive malware issues, "business continuity planning and testing activities should incorporate response and recovery capabilities and test resilience against cyber-attacks involving destructive malware."[35] In addition to the list noted above for the Joint Statement on Cyberattacks Compromising Credentials, the Joint Statement on Destructive Malware indicates that institutions should also:

- Securely configure their systems and services; and
- Review, update, and periodically test their incident response and business continuity plans.

In addition to the various FFIEC guidance applicable to national banks and federal thrifts, the OCC has promulgated guidance regarding its expectation that "banks [and thrifts] should have risk management programs to identify and appropriately consider new and evolving threats to online accounts and to adjust their customer authentication, layered security, and other controls as appropriate in response to changing levels of risk."[36] The OCC expects financial institutions to report cyberattacks to law enforcement authorities and to their supervisory regulators, as well as voluntarily file SARs if the attacks affect the institution's critical information or other critical systems. According to OCC guidance, financial institutions should heighten their awareness of attacks, employ appropriate resources to identify and mitigate risks, ensure appropriate personnel is involved in incident response, incorporate information sharing with other institutions into their risk mitigation strategies, and be prepared to provide timely communications to customers. According to the OCC, an institution's cyberattack preparation and mitigation strategies should apply and extend on an enterprise-wide basis.

…"banks should have risk management programs to identify and appropriately consider new and evolving threats to online accounts and to adjust their customer authentication, layered security, and other controls as appropriate in response to changing levels of risk."

In addition to the promulgation of guidance specific to cybersecurity programs, FBAs are increasingly considering a financial institution's cybersecurity measures as part of the institution's BSA/AML compliance obligations. In a recent speech on March 2, 2015 before the Institute of International Bankers, OCC Comptroller Curry stated that "the goals of BSA/AML and cybersecurity are increasingly converging. Terrorists, drug cartels, and cybercriminals all have a need to generate cash and move money, and it would seem that many of them would share some of the same goals. There are lessons to be learned from our decades-long experience in BSA enforcement that can be applied to the cybersecurity area, and vice versa."[37] Financial institutions

should expect increased FBA supervision of their cybersecurity measures, including as part of regulatory examinations.

…"the goals of BSA/AML and cybersecurity are increasingly converging…There are lessons to be learned from our decades-long experience in BSA enforcement that can be applied to the cybersecurity area, and vice versa." Thomas Curry, Comptroller of the Currency

Risks and Consequences

Clearly, depository institutions of all sizes must make a significant commitment of resources, time and money to address the growing threat of cyber risks, and some institutions are experiencing adverse examination ratings on areas such as earnings, management and potentially even capital as a result of the inability to control and contain escalating compliance costs related to cybersecurity issues. In addition to this regulatory/supervisory "catch 22" of trying to balance heightened compliance demands requiring additional resources versus the financial impact on an institution from the cost of such resources, are the following issues of which banks and other depository institutions must be mindful:

- **Consumer Litigation –** ACH and wire-related fraud incidents continue to grow at an alarming pace. Identity theft and breaches of consumer privacy expose financial institutions to a significant risk of consumer litigation. For example, in 2014, a county hospital sued a large national bank to recoup losses from a cyber-heist in which cyber thieves broke into the hospital's payroll accounts and put through three unauthorized ACH payments, siphoning over $1 million. The hospital sued the national bank for processing an unauthorized transfer request, arguing breach of a contractual provision incorporating the NACHA rules, which require the bank to implement a risk management program. The case is currently pending.[38]

- **Compliance Risks –** The pace of new regulatory requirements can challenge the change-management capabilities of some financial institutions and lead to increased operational and compliance risks if banks do not adequately invest in control processes, systems, or staff. Institutions may be cited for weak cybersecurity systems and inadequate controls as part of an overall operational risk review. Of particular concern is the likelihood that the industry will see increased enforcement actions given increased regulatory concerns over data privacy and cyberterrorism.

- **Operating Risks –** Data breaches arising from a cyberattack can also lead to the loss of critical confidential commercial or financial information, significant operational dysfunction, and the theft of sensitive internal documents such as technical papers, R&D reports, and other communications.

- **Conflicting Obligations –** In some cases, law enforcement authorities may request financial institutions to not take action to stop a cyber-breach in order to provide an opportunity for law enforcement officials to catch the cyber criminals. In fact, financial institutions regularly cooperate with law enforcement agencies to facilitate law enforcement's "sting" type operations. In some cases, however, a risk-averse financial institution may prefer immediately to shut down access to systems and assess the damage to protect consumers and thereby limit the institution's own liability. Because governmental entities' ability to indemnify a financial institution is often limited, financial institutions could also find themselves on the hook for potential damages in cases where law enforcement investigations go awry.

- **Reputational Risk –** Data breaches expose customers to an increased risk of identity theft and loss of privacy, which will result in loss of confidence in a financial institution's security systems and in the financial institution itself. Not only can a cyberattack damage an institution's relationship with its customers, but the negative publicity surrounding a breach can have long-term impacts. A successful cyberattack not only can lead to loss of business, but can expose the financial institution to consumer litigation, regulatory enforcement actions, and even criminal investigations, all of which will further exacerbate damage to the institution's reputation.

- **Fines and Penalties –** Another significant concern is the possibility that a cyberattack could lead to the imposition of regulatory, civil and/or criminal fines and penalties arising from the failure of a depository institution to maintain an adequate cybersecurity program, which thereby results in a customer data breach.

- **Cyber Costs and Benefits –** There are numerous additional costs and benefits that institutions must consider in the new world of cyber risks and vulnerabilities. One cost that many institutions are now taking on involves cyber insurance policies that can help to mitigate some of the costs and liabilities created by cyberattacks and data breaches. Where traditional insurance policies are insufficient, specialized cyber insurance policies now cover data breaches, identity theft, loss of data, business interruption, cyber extortion, crisis management, and other cyber-risk areas. As with any other significant cost decision, institutions must carefully weigh the extent of the additional insurance and whether the cost is justified based on the additional insurance protection provided under a particular cyber insurance policy.

A successful cyberattack not only can lead to loss of business, but can expose the financial institution to consumer litigation, regulatory enforcement actions, and even criminal investigations, all of which will further exacerbate damage to the institution's reputation.

- **Third-Party Risk Management –** An area of particular concern to bank regulators is the exposure and vulnerability of banks to third party service providers that may not be adequately prepared or equipped to address their own cyber-security vulnerabilities and, thus, may wittingly or unwittingly act as a Trojan horse to expose banks to new cyber-risks. This is a critical compliance issue for all institutions in today's complex information technology environment. In a report released earlier this month, NYDFS noted that vendors may sometimes provide a "backdoor entrance" for hackers seeking to steal sensitive bank customer data. Key report findings include:

  – Nearly 30% of banks surveyed by the NYDFS did not require third-party vendors to notify them of cybersecurity breaches;

  – Over half of the banks surveyed did not conduct on-site assessments of their third party vendors;

  – One in five banks surveyed by the NYDFS did not require third-party vendors to represent that they have established minimum information security requirements; and

  – Nearly half of the banks surveyed did not require a warranty of the integrity of a vendor's data or products.

- **Impact on Smaller Institutions –** Larger banks generally have sophisticated IT systems to guard against cyberattacks. By contrast, smaller community-based banks generally lack such systems and, therefore, are often a prime target for cyber thieves. Understanding this vulnerability, the FBAs are seeking to make sure that bankers have integrated cybersecurity systems into their operations. However, many institutions, particularly smaller community-based institutions, have yet to face a full-blown cyberattack and, thus, may not fully appreciate the extent of the risk. This remains a significant industry challenge.

Nearly 30% of banks surveyed by the NYDFS did not require third-party vendors to notify them of cybersecurity breaches…

Maintain an Effective Data Breach Response Program

At minimum, an institution's data breach response program should include procedures for:

- **Identification Procedures –** Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused.
- **Notification Procedures –**
  - Notifying the primary federal (and state) regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
  - Notifying customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it; and
  - File a timely Suspicious Activity Report ("SAR"), and in situations involving federal criminal violations requiring immediate attention, e.g., an active event, promptly notify law enforcement authorities; and
  - When an incident of unauthorized access to sensitive customer information involves customer information systems maintained by an institution's third party service provider, it is important to remember that it is the financial institution's responsibility to notify its customers and regulator.
- **Remediation Procedures –** Taking appropriate steps to contain and control a cyberattack involving a breach incident to prevent further unauthorized access to or use of customer information.

Best Practices to Prevent and Mitigate Attacks and Data Breaches

At minimum, a financial institution's data breach response program should contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;

- Consistent with the financial institution's obligation to file a SAR, filing a timely SAR, and considering voluntarily filing a SAR when circumstances warrant;
- In situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities;
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- Notifying customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it, and providing support services—such as free credit monitoring—to consumers affected by a breach.

Additionally, financial institutions should consider implementing the following best practices:

- **Create and/or review your plan periodically –** If your financial institution does not already have a plan in place to deal with data breaches and/or other cybercrime, evaluate the institution's priorities and prepare a plan to initiate if an event occurs. Because of the high levels of risk associated with cybercrime, it is critical to identify and neutralize threats immediately, as well as take appropriate steps to mitigate damage.
- **Assemble an internal team –** Your financial institution should also identify a team with security expertise and designate decision making authority to the team in the event an attack occurs. The team should be led by a single individual, who can act as a point of contact for directors, officers, employees, and third parties and streamline the process of dealing with the ramifications of an attack.
- **Secure outside counsel –** If your financial institution has not already done so, seek and retain outside counsel with expertise in dealing with cyberattacks and related issues, including regulatory compliance, privacy, and consumer protection issues. Additionally, your institution should identify and be prepared to engage other industry experts to provide advice and expertise in the event of a cyberattack.
- **Monitor and update information security systems –** Recent cyberattacks have demonstrated the ability of cybercriminals to rapidly evolve and shift cyberattack methods. You should anticipate that protection software that is currently effective may not remain effective for long. To protect your financial institution, you should monitor and periodically test your software and other preventative measures to ensure continued effectiveness.
- **Train employees –** Your financial institution should provide cybersecurity awareness training to its employees, including training employees on safe internet and internal system practices, as well as training to recognize and not open suspicious emails, and to identify and report unusual customer transactions. Strong employee training can reduce risk of cyberattacks, as inadvertent downloads by employees is one of the main ways cybercriminals gain access to financial institution's internal systems.
- **Prepare a strategy to address the problems –** Even with a thorough action plan in place prior to an incident, financial institutions must be prepared to respond appropriately to a specific incident once it occurs. For example, your financial institution may have various

iterations of its action plan for different levels of cybercrime events (i.e., a single database breach vs. institution-wide infiltration of IT systems). Your institution should be prepared to amend its action plan as necessary to deal with specific threats.

- **Be prepared to brief regulators and law enforcement on the incident –** In connection with your legal team and other experts, your financial institution should obtain as much information as possible in the wake of a cybercrime event. This includes information about the crime itself, as well as the steps the institution has taken and plans to take to mitigate damage.

- **Practice the plan and engage the plan immediately in the event of an incident –** Your financial institution and its employees should be well-rehearsed in putting the institution's response and action plan into effect once a cybercrime has occurred. In responding to a cyberattack, time is of the essence, both in terms of mitigating damage to the financial institution, and in dealing with potential backlash from customers and/or the public. Because a delay in responding to an attack may be viewed as the result of lack of preparation or indecisiveness—or worse, incompetence—on the part of an institution's directors and officers, it is critical that your institution be prepared to respond swiftly and decisively in the event of a cyberattack.

Paul Hastings lawyers regularly advise clients regarding cybersecurity issues.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Todd W. Beauchamp
1.404.815.2154
toddbeauchamp@paulhastings.com

Chris Daniel
1.404.815.2217
chrisdaniel@paulhastings.com

Erica Berg Brennan
1.404.815.2294
ericaberg@paulhastings.com

Heena A. Ali
1.404.815.2393
heenaali@paulhastings.com

Kevin P. Erwin
1.404.815.2312
kevinerwin@paulhastings.com

Meagan E. Griffin
1.404.815.2240
meagangriffin@paulhastings.com

Diane Holden
1.404.815.2326
dianeholden@paulhastings.com

London

Ben Regnard-Weinrabe
44.020.3023.5185
benregnardweinrabe@paulhastings.com

Nikki Johnstone
44.020.3023.5112
nikkijohnstone@paulhastings.com

Miah Ramanathan
44.020.3023.5178
miahramanathan@paulhastings.com

Palo Alto

Cathy S. Beyda
1.650.320.1824
cathybeyda@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Stan Koppel
1.415.856.7284
stankoppel@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Ryan M. Decker
1.415.856.7237
ryandecker@paulhastings.com

Molly E. Swartz
1.415.856.7238
mollyswartz@paulhastings.com

Washington, D.C.

V. Gerard Comizio
1.202.551.1272
vgerardcomizio@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

Gerald S. Sachs
1.202.551.1975
geraldsachs@paulhastings.com

Alexandra L. Anderson
1.202.551.1969
alexandraanderson@paulhastings.com

Laura E. Bain
1.202.551.1828
laurabain@paulhastings.com

Katie A. Croghan
1.202. 551-1849
katiecroghan@paulhastings.com

Ryan A. Chiachiere
1.202.551.1767
ryanchiachiere@paulhastings.com

Lauren Kelly D. Greenbacker
1.202.551.1985
laurenkellygreenbacker@paulhastings.com

Amanda Kowalski
1.202.551.1976
amandakowalski@paulhastings.com

[1] Kaspersky Lab, Carbanak Apt The Great Bank Robbery 3 (February 2015), *available at* http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf.

[2] Communications-Electronics Security Group of the UK Government, Common Cyber Attacks: Reducing the Impact (2015), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf.

[3] OCC, Information Security: Distributed Denial of Service Attacks and Customer Account Fraud (Dec. 21, 2012), *available at* http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html.

[4] Communications-Electronics Security Group of the UK Government, Common Cyber Attacks: Reducing the Impact (2015), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf.

[5] Kaspersky Lab, Carbanak Apt The Great Bank Robbery 3 (February 2015), *available at* http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf.

[6] Mike Lennon, *Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kapersky Lab,* SECURITYWEEK (Feb. 15, 2014), *available at* http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

[7] Kaspersky Lab, Carbanak Apt The Great Bank Robbery 3 (February 2015), *available at* http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf.

[8] Kaspersky Lab, Carbanak Apt The Great Bank Robbery 3 (February 2015), *available at* http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf.

[9] Mike Lennon, *Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kapersky Lab,* SECURITYWEEK (Feb. 15, 2014), *available at* http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

[10] Mike Lennon, *Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kapersky Lab,* SECURITYWEEK (Feb. 15, 2014), *available at* http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab.

[11] Ina Paiva Cordle, *TotalBank responds to computer security breach*, MIAMI HERALD (Aug. 7, 2014), *available at* http://www.miamiherald.com/news/business/article1978822.html.

[12] Emily Glazer, *J.P. Morgan's Cyber Attack: How the Bank Responded,* WSJ (Oct. 3, 2014), *available at* http://blogs.wsj.com/moneybeat/2014/10/03/j-p-morgans-cyber-attack-how-the-bank-responded/.

[13] Penny Crossman, *Is Apple Pay a Fraud Magnet? Only If Banks Drop the Ball,* American Banker, Bank Technology News (March 5, 2015), *available at* http://www.americanbanker.com/news/bank-technology/is-apple-pay-a-fraud-magnet-only-if-banks-drop-the-ball-1073127-1.html.

[14] Comments of Samuel Bucholtz, co-founder, Casaba Security, on CNBC (March 4, 2015).

[15] Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (February 13, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[16] U.S. Department of the Treasury, Press Release (Apr. 1, 2015), *available at* http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150401.aspx.

[17] Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," (Apr. 1, 2015), *available at* http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.

[18] The Protecting Cyber Networks Act (H.R. 1560), *available at* http://intelligence.house.gov/ProtectingCyberNetworksAct; *see also* Michael S. Schmidt, Computer Attacks Spur Congress to Act on Cybersecurity Bill Years in the Making, New York Times (April 22, 2015), *available at* http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html.

[19] The National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1731; *see also* Cory Bennett & Cristina Marcos, House Passes

Cybersecurity Bill, The Hill (April 22, 2015), *available at* http://thehill.com/blogs/floor-action/house/239756-house-passes-cybersecurity-bill.

[20] *'Cyber attack war games' to be staged by UK and US,* BBC (Jan. 16, 2015), *available at* http://www.bbc.com/news/uk-politics-30842669.

[21] *See* NCCIC Overview, *available at http://www.dhs.gov/about-national-cybersecurity-communications-integration-center*.

[22] Kaja Whitehouse, *Regulator warns of 'Armageddon' cyber attack on banks,* USA TODAY (Feb. 25, 2015), *available at* http://www.usatoday.com/story/money/business/2015/02/25/lawsky-goldman-sachs-banks/23995979/.

[23] Kaja Whitehouse, *Regulator warns of 'Armageddon' cyber attack on banks,* USA TODAY (Feb. 25, 2015), *available at* http://www.usatoday.com/story/money/business/2015/02/25/lawsky-goldman-sachs-banks/23995979/.

[24] The FBAs are the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Federal Reserve Board of Governors.

[25] OCC Semiannual Risk Perspective Report (Spring 2013), *available at http://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2013.pdf*.

[26] Comments of Sarah J. Dahlgren, Executive Vice President, Federal Reserve Bank of New York at the OpRisk North America Annual Conference, March 24, 2015, *available at* http://www.bis.org/review/r150325b.htm.

[27] FFIEC Cybersecurity Assessment General Observations (2014), *available at* http://www.ncua.gov/Resources/CUs/Documents/FFIEC_Cybersecurity_Assessment_Observations.pdf.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] FFIEC Cybersecurity Assessment General Observations (2014), *available at* http://www.ncua.gov/Resources/CUs/Documents/FFIEC_Cybersecurity_Assessment_Observations.pdf.

[32] FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement (Nov. 2014), *available at* https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf.

[33] *Available at* http://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf.

[34] *Available at* http://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf.

[35] *Id.*

[36] OCC, Information Security: Distributed Denial of Service Attacks and Customer Account Fraud (Dec. 21, 2012), *available at* http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html.

[37] Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Institute of International Bankers (Mar. 2, 2015), *available at* http://www.occ.gov/news-issuances/speeches/2015/pub-speech-2015-32.pdf.

[38] *Hospital Sues Bank of America Over Million-Dollar Cyberheist*, Krebs on Security (Mar. 3, 2015), *available at* https://krebsonsecurity.com/2015/03/hospital-sues-bank-of-america-over-million-dollar-cyberheist/.