Skadden

PRIVACY & CYBERSECURITY UPDATE

FEBRUARY 2015

CONTENTS (click on the titles below to view articles)

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 14, or your regular Skadden contact.

WHITE HOUSE RELEASES PROPOSED PRIVACY LEGISLATION

President Obama has proposed federal privacy legislation that would require companies to meet certain minimum privacy standards for consumers. The proposal includes a "safe harbor" for companies that comply with industry codes of conduct that is likely to concern privacy advocates.

On February 27, the White House released its proposal for federal privacy legislation. The proposed act — the Consumer Privacy Bill of Rights — is part of the suite of cybersecurity and privacy initiatives that President Barack Obama announced in January. We outline below the key points of the proposal,[1] which now needs a legislative sponsor in Congress:

- **Covered Entities.** The act would cover any entity that collects, creates, process, retains, uses or discloses personal data in interstate commerce (Covered Entities) with certain exclusions for small companies
- **Notice.** Covered Entities would be required to provide concise, easily understandable and conspicuous notice about their privacy and security practices, which must be reasonable "in light of the context." The notice must include, among other things, the data being collected, the purpose for which it is being used, and any person or entities to whom the data will be disclosed. Companies would need to consider the size of the device on which the notice appears and how often it is displayed to consumers.
- **Individual Control.** The proposed act provides that individuals would have the right to "control" the processing of their personal data "in proportion to the privacy risk to the individual and consistent with the context." Individuals would, for example, have the right to withdraw their consent from having their data processed. The Covered Entity could then delete the data or de-identify it. In a clear swipe at the EU's recent ruling on the right to be forgotten (under which individuals can ask that search results about their prior history be deleted),[2] the proposed act states that a Covered Entity would not have to delete the data if it has an applicable First Amendment Interest keep it.
- **Respect for Context.** The proposed act establishes a vague concept of "context": If a Covered Entity processes data "that is not reasonable in light of the context," it should conduct a "privacy risk analysis" and address any risks uncovered, through steps such as heightened transparency and individual control. This would entail providing reasonable notice to individuals, given the context, to allow them to reduce their privacy risk. As part of the analysis, Covered Entities would need to examine any disparate impact on specific groups, a step that is likely fostered by concerns over how big-data analytics might unfairly impact minority groups.
- **Privacy Review Boards.** A Covered Entity could process data in a manner "that is not reasonable in light of the context" if it is supervised by an FTC-approved "Privacy Review Board." The boards would determine if heightened transparency and individual control is not practical, whether such processing has "substantial benefits" that outweigh the privacy risks and if the Covered Entity took reasonable steps to mitigate the risks.

[1] The proposed bill can be found at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[2] For more on the "right to be forgotten," see Skadden's November 2014 *Privacy & Cybersecurity Update*.

- **Data Collection and Responsible Use.** Covered Entities are directed to only collect, retain, and use personal data in a manner that is "reasonable in light of the context," and should seek to "minimize privacy risks."
- **Data Destruction.** Covered Entities would be required to delete, destroy or de-identify any personal data within a reasonable time after it was no longer required for its original purpose.
- **Security.** Covered Entities would be required to identify reasonably foreseeable security risks, and implement maintain safeguards reasonably designed to ensure the security of personal data. This includes protecting against unauthorized loss, misuse, destruction and access. The reasonableness of the steps taken would be assessed based on the degree of privacy risk, the foreseeability of threats, "widely accepted practices in administrative, technical, and physical safeguards for protecting personal data," and cost.
- **Access and Accuracy.** Covered Entities would have an obligation to provide individuals with access to their data in most cases, use reasonable efforts to ensure the data is accurate and correct any errors identified by the individual.
- **Accountability.** Covered Entities would need to provide privacy training to employees, conduct internal or independent audits of their privacy protections, and adopt "privacy by design" programs.
- **Enforcement.** The FTC is designated to enforce the proposed act under its Section 5 powers but cannot bring an enforcement action during the first 18 months after an entity starts to create or process personal data. State Attorneys General also can bring actions under the proposed act, but only for injunctive relief. However, the attorney general must provide the FTC with 30 days' advanced notice of initiating an action, and the FTC can elect to assume lead responsibility.
- **Potential Penalties.** In addition to injunctive relief, the act allows the FTC to seek civil penalties of $35,000 per day of violation, which increases to $50,000 per day if the violator is on notice. Civil penalties would be capped at $25 million.
- **Safe Harbor Protection.** Undoubtedly one of the most controversial aspects of the proposed act is the availability of "safe harbor" protection for following industry codes of conduct. Under the proposal, groups — including those formed by the Department of Commerce — can ask the FTC to approve a code of conduct that provides equivalent or greater protection of personal data. The request also must specify the process through which the code was developed (which must be transparent) as well as the entities covered by that code. Codes of conduct that are approved must be reassessed by the FTC between three and five years after adoption. Covered Entities charged with violating the act would have immunity if they demonstrate that, with respect to the violation, they "maintained a public commitment to adhere to a Commission-approved code of conduct.
- **Preemption.** The act would preempt all state privacy laws, with limited exceptions, including for laws dealing with financial and health information, or personal information of minors.

OBSERVATIONS

The proposed Act is already being criticized by all factions, including those who think it goes too far in impacting businesses' freedom to operate and those who believe it does not offer sufficient privacy protection. Privacy advocates will be especially concerned about the Safe Harbor option, and that the FTC was not granted any rulemaking authority to enhance existing privacy laws. States have balked at having their privacy laws preempted by federal legislation.

Moreover, much of the legislation offers vague standards that companies and consumers will struggle with. For example, it will be difficult to define the collection of data in a manner that is "reasonable in light of the context." Companies also will object to the very loose and ambiguous data security requirements.

We anticipate that the proposed act, like much privacy legislation before it, will face an uphill battle in Congress and likely not be enacted as currently drafted.

Return to Table of Contents

LESSONS FROM THE ANTHEM DATA BREACH

The Anthem data breach highlights the growing pressure to notify consumers quickly in the event of a data breach and the need for strong cybersecurity governance and a Security Incident Response Plan.

On February 4, Anthem Inc., one of the nation's largest health insurers, announced that it had been the victim of a sophisticated cyberattack in which hackers were able to gain access to a database containing the data of tens of millions of current and former Anthem customers and employees. Anthem, which operates under a number of different brands, including Anthem Blue Cross and Blue Shield, reported that the data included names, dates of birth, addresses, Social Security numbers, emails, employment information and certain income data, though reportedly no credit card or medical information. The attack is one of the largest breaches of customer information to date, with approximately 80 million records accessed. In its announcement, the company said it planned to begin individually notifying plan members in coming weeks and will offer credit monitoring and identity protection services to those affected.

The Anthem incident provides yet another example of what companies can expect in the aftermath of a cyberattack. Less than a day after Anthem announced the cyberattack, class actions were filed in California, Indiana and Alabama federal courts under claims of negligence, invasion of privacy, violations of state laws and other causes of action. The lawsuits allege Anthem did not have proper security procedures in effect, waited too long to tell customers about the breach (the breach was discovered on January 29) and failed to properly encrypt user data. As of February 18, more than 24 putative class actions had been filed. One Anthem customer has asked the U.S. Judicial Panel on Multidistrict Litigation to consolidate 17 of those class actions in Indiana, the location of Anthem's headquarters, arguing that the actions raise common allegations and questions of fact about Anthem's security procedures.

Several states and federal agencies have also begun investigations into the Anthem attack. The state investigations plan to examine Anthem's security practices and privacy policies, whether Anthem heeded warnings about vulnerabilities in its systems and whether Anthem should have had stronger security measures in place. The Department of Health and Human Services inspector general's office announced that it is working in conjunction with the FBI to determine whether the personal information of Medicare and Medicaid beneficiaries was accessed. The Anthem attack has highlighted that HIPAA does not require encryption of member data, a fact many have expressed concern about.

While many consider Anthem to have acted in a prompt manner — and indeed the FBI praised Anthem for its quick response — a February 10 letter sent by the Connecticut Attorney General on behalf of attorneys general from Arkansas, Illinois, Kentucky, Maine, Mississippi, Nebraska, Nevada, Pennsylvania and Rhode Island expressed concern with Anthem's delay in notifying those affected and providing the credit monitoring services it had promised. The letter also asked Anthem to compensate consumers for any losses associated with the breach

during the period between the date of the breach and the date Anthem provided consumers with access to credit and identity theft safeguards.

PRACTICE POINTS

The Anthem data breach highlights the importance of implementing strong cybersecurity governance and conducting a cybersecurity audit to determine how cybersecurity is managed and messaged within an organization. It is noteworthy that the state investigations are focused on this aspect of the breach, and it likely that plaintiffs' counsel will be as well.

The Connecticut AG letter is yet another example of how states are increasingly focused on the speed of data breach notification, and that delays of even just a few days may not be tolerated. The fact that the AGs requested that Anthem compensate consumers for losses during the period between the date of the breach and the date identity theft safeguards were offered adds another type of exposure for companies. The Anthem data breach therefore highlights the critical importance of developing and testing a Security Incident Response Plan (SIRP). In our experience, companies respond more efficiently and effectively to a cyberattack when a well-tested SIRP is in place.

Return to Table of Contents

SEC AND FINRA RELEASE RESULTS OF INDUSTRYWIDE CYBERSECURITY EXAMINATION SWEEPS

The SEC and FINRA have released results of their cybersecurity examinations of broker-dealers and investment advisers. Their findings may be helpful to organizations, regardless of industry, looking to enhance their own cybersecurity measures.

On February 3, the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) each released the results of their own cybersecurity examination sweeps. The SEC conducted exams of broker-dealers and investment advisers while the FINRA report was limited to broker-dealers. The findings detail the level of preparedness among firms examined and provide a useful guide for organizations seeking to bolster their own cybersecurity.

SEC RISK ALERT AND ONGOING CYBERSECURITY INITIATIVES

The SEC's Office of Compliance Inspections and Examinations published a Risk Alert[3] summarizing the findings of its recent cybersecurity examination sweep of 57 registered broker-dealers and 49 registered investment advisers conducted in connection with the SEC's Cybersecurity Initiative (the Initiative).[4] The exams were conducted in order "to better understand how firms are addressing the legal, regulatory, and compliance issues associated with the (Initiative)."

The Risk Alert states that:

- The vast majority of firms examined (1) have adopted written information security policies, (2) conduct periodic risk assessments on a firmwide basis to identify cybersecurity threats, vulnerabilities and potential business consequences, and (3) conduct firmwide inventorying, cataloguing or mapping of their technology resources.

[3]The full text of the Risk Alert is available at http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
[4]For a more in-depth discussion of the Initiative, see page 3 of our April 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_April_2014.pdf.

- Most of the examined firms reported that they have been the subject of a cyber-related incident.
- Over half the broker-dealers and just under half the advisers reported receiving fraudulent emails seeking to transfer client funds, some of which resulted in losses.
- Many examined firms identified best practices through information-sharing networks.

The SEC also reviewed firm cybersecurity policies relating to vendors and business partners, use of encryption technology, designation of a chief information security officer and use of cybersecurity insurance. In almost all categories, a greater percentage of broker-dealers had policies or procedures in place to address areas of concern than did investment advisers.

Exams were conducted through document reviews and interviews with key firm personnel, to "discern basic distinctions among the level of preparedness of the examined firms." The Risk Alert notes that the examined firms were chosen in order to provide a cross-section of the industry and "to assess various firms' vulnerability to cyber-attacks." SEC staff is continuing to review information gathered as a result of the exams.

The SEC's National Exam Program Examination Priorities for 2015 include, again, cybersecurity as an exam priority,[5] and on February 4, Vincente Martinez, chief of the Office of Market Intelligence in the SEC's Enforcement Division, indicated at the FINRA/SIFMA Cybersecurity Conference that the SEC will conduct additional exams focusing on IT controls of a smaller group of firms. The Risk Alert notes that the SEC "will continue to focus on cybersecurity using risk-based examinations."

FINRA CYBERSECURITY REPORT

FINRA has published the results of its Report on Cybersecurity Practices[6] (the Report) and an accompanying Investor Alert[7] on cybersecurity practices in an effort to help broker-dealers better prepare for and respond to threats posed by cyberattacks. FINRA conducted targeted examinations of a cross-section of broker-dealers throughout 2014 and interviewed organizations involved with cybersecurity to understand the threats firms face and how firms are dealing with those threats, and to share these observations with other firms.

FINRA's Investor Alert encourages investors to become familiar with their brokerage firms' cybersecurity policies and provides key questions the investors are encouraged to ask the firm regarding safeguards and reimbursement policies in the event assets are compromised in an attack.

The Report identifies principles and effective practices, grounded in risk management, while recognizing that no single approach will work for all firms. Significantly, the Report provides a thorough road map of what steps FINRA expects firms to be taking with respect to cybersecurity protection. This road map is also useful for any company in any industry that is seeking a guide on "best practices" in the area of cybersecurity preparedness.

The Report highlights the following critical steps:

- Conducting a **risk assessment** to understand the cybersecurity risks a company faces across all activities and assets;
- Instituting a **strong governance** framework with strong leadership at the board and senior management levels;

---

[5]The SEC's "Examination Priorities for 2015" (Jan. 13, 2015), is available at http://www.sec.gov/news/pressrelease/2015-3.html.

[6]The full text of the FINRA report is available at https://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p602363.pdf.

[7]The Investor Alert is available at https://www.finra.org/Investors/ProtectYourself/InvestorAlerts/MoneyManagement/P601655.

- Implementing **technical controls**, including a "defense-in-depth" approach;
- Developing, implementing and testing **incident response plans** (which should include steps toward containment, mitigation, eradication, recovery, investigation, notification and making customers whole);
- Undertaking strong diligence and **management of vendor relationships**;
- Conducting **effective training** to certain staff about cybersecurity risks;
- Participating in **intelligence-sharing opportunities**; and
- Obtaining **cyber insurance**.

The key takeaways from the Report are as follows:

- While the Report lists "technical controls" as a necessary step for every company to take and provides some general guidance, FINRA acknowledges that there are numerous technology options available, and every company must make its own decisions in this regard. We believe that regulators will continue to follow this approach, and rarely suggest specific technology steps companies must take. Instead, the focus will continue to be on governance, process and general non-IT cybersecurity preparedness.
- The Report's focus on strong leadership, including board- and senior-level engagement, on cybersecurity issues highlights the importance of adopting a top-down approach to cybersecurity. Internal reporting and established governance processes are critical for every company to adopt.
- Many companies design cybersecurity plans in a vacuum without first analyzing the specific risks their organization faces. As the Report makes clear, a comprehensive risk assessment is an important starting point in any cybersecurity plan. FINRA outlined some of the key steps in this regard, including:
  - dentifying and maintaining an inventory of assets that can access the firm's network;
  - Assessing external and internal threats and asset vulnerabilities; and
  - Prioritizing recommendations to remediate identified risks.
- The Report provides useful guidance on the role of board members. Specifically, the Report cites the five cybersecurity principles outlined by the National Association of Corporate Directors (NACD):
  - Directors need to understand and approach cybersecurity as an enterprisewide risk management issue, not just an IT issue;
  - Directors should understand the legal implication of cyber risks as they relate to their company's specific circumstances;
  - Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda;
  - Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget; and
  - Board and management discussion of cyber risks should include identification of which risks to avoid, accept, mitigate or transfer through insurance, as well as specific plans associated with each approach.
- FINRA recommends that organizations establish a common framework and vocabulary when discussing cybersecurity and cyberattacks. We believe this is a best practice. All too often, companies trying to deal with a cybersecurity issue find that different internal stakeholders

have different criteria for what constitutes an incident or a remediation plan. This can lead to confusion and miscommunication at the critical time when an attack is unfolding.

- FINRA also recommends developing, implementing, monitoring and updating metrics to measure a firm's cybersecurity performance. We find that this is an often overlooked area of cybersecurity preparedness. Without some type of metric, companies are hard-pressed to adequately evaluate whether their cybersecurity program is achieving its stated goals, and whether necessary improvements are taking place.

PRACTICE POINTS

In light of the SEC's and FINRA's continued focus on cybersecurity and a series of high-profile corporate data breaches, registered broker-dealers and registered investment advisers should continue to review or prepare their cybersecurity policies, procedures and preparedness. More generally, the FINRA report provides a comprehensive overview of cybersecurity preparedness that is applicable to any company, regardless of industry.

Return to Table of Contents

COSO RELEASES REPORT ON ASSESSING AND RESOLVING CYBER RISKS

COSO has released a report that details how organizations can use its existing internal control framework to assess and resolve the risks of a cyberattack.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a joint initiative of five private sector organizations,[8] recently released a report advising companies how to assess and resolve cyber risks. Established in 1985, COSO aims to provide guidance to business and government entities through the development of frameworks and suggestions related to enterprise risk management, internal control and fraud deterrence. COSO is influential across a range of industries, and its frameworks have been adopted by both government and business entities.

In January, COSO released a report that it commissioned from Deloitte & Touche LLP, which details the ways in which organizations can use the COSO Internal Control-Integrated Framework (2013 Framework) to assess and resolve cyber risks.[9] The 2013 Framework provides principles-based guidance for designing and implementing effective internal controls. COSO, which designed the first Internal Control-Integrated Framework in 1992 in response to senior executives' need to optimally control their enterprises, updated the framework to offer organizations ways to use and manage technology for internal control purposes. One of COSO's primary goals in revising the 2013 Framework was to reflect how globalization and technology have changed both how companies operate and the type and degree of challenges businesses face (*e.g.*, online information security vulnerability).

The 2013 Framework is structured around 17 internal control principles that fit into the five broad components of internal control: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities.[10] Though the components operate together in an integrated manner, each one is a lens through which organizations can assess their existing cyber infrastructure to identify priorities, strengths and weaknesses.

---

[8] The five co-sponsors are: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA) and the National Association of Accountants (now the Institute of Management Accountants [IMA]).

[9] The "COSO in the Cyber Age" report is available at http://www.coso.org/documents/coso%20in%20the%20cyber%20age_full_r11.pdf.

[10] For a description of the 17 principles, see the "Internal Control — Integrated Framework" (2013), available for purchase at http://www.coso.org/ic.htm.

In relation to each component of internal control, the COSO report suggests that the board of directors and audit committees consider the following:

(1) Control Environment

- Do they understand the organization's cyber risk profile?
- Are they informed as to how the organization currently manages cyber risks?

(2) Risk Assessment

- Have they evaluated the organization's operations, reporting and compliance objectives?

(3) Control Activities

- Has the organization developed control activities, including with respect to technology?
- Are there formal policies in place around any such control activities?

(4) Information and Communication

- Have they identified information requirements to manage cyber risks?
- Have they established communication protocols to facilitate internal control over cyber risks and attacks?

(5) Monitoring Activities

- Is there an existing monitoring program in place to assess the organization's current cyber risk management system?
- How can the organization analyze and improve its cyber risk policies and profile?

These internal control components offer a prism through which organizations can identify the business' key objectives, critical information systems and related risk tolerance levels. The report notes that cyber risks cannot be mitigated to zero, but companies can use the 2013 Framework to prioritize their cyber risk management resources in an informed manner.

Return to Table of Contents

WHITE HOUSE ANNOUNCES NEW CYBER THREAT INFORMATION SHARING AGENCY

A new government agency will facilitate the sharing of cybersecurity threat information among government agencies and develop actionable intelligence.

On February 10, the White House announced its intention to create the Cyber Threat Intelligence Integration Center (CTIIC), a new agency designed to facilitate sharing of cybersecurity threat information among government agencies. In a speech at the Wilson Center in Washington, D.C., Lisa Monaco, assistant to the president for homeland security and counterterrorism, said the new agency will be designed to rapidly collect, analyze and distribute data on cybersecurity incidents within the federal government. Monaco suggested the agency would be modeled after the National Counterterrorism Center (NCTC), which was created to facilitate similar interagency information sharing in the wake of the September 11 attacks.

Monaco identified recent threats to the U.S. private sector as a spur to the creation of the new agency, specifically noting that the recent hacking of Sony Pictures was "a game changer."[11]

[9]For more information on the Sony attack, see our December 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_December_2014.pdf.

According to Monaco, it had been difficult to obtain a clear consensus on the impact of the attack and the parties responsible, in part because of conflicting views among the different agencies responsible for national cyberdefense. The plan is for CTIIC to serve as a neutral party responsible for synthesizing information from multiple agencies into actionable intelligence without favoring any one source.

CTIIC now joins several existing government centers dedicated to collecting and analyzing cybersecurity threat information. As we reported in our December 2014 *Privacy & Cybersecurity Update*, the National Cybersecurity Protection Act of 2014 recently codified the authority of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC), which serves as a federal-civilian interface for cross-sector information sharing. The FBI's Cyber Division has also increased its efforts to reach out to the private sector to collaborate on cybersecurity incident investigations and response through programs such as InfraGard, a cybersecurity data-sharing organization.[12]

As NCCIC, the FBI and other agencies are already responsible for collecting and sharing cybersecurity information inside and outside of the federal government, some have questioned the utility of adding another layer of information-sharing bureaucracy. Some members of the House and Senate have also expressed concern that they were not appropriately briefed by the White House on the new center and have intimated that CTIIC funding may not be guaranteed. Given the successes of NCTC in the counterterrorism arena and the threat posed by cyberattacks, however, the White House believes CTIIC is necessary to address the current gaps in intelligence assessments of cybersecurity threats.

Return to Table of Contents

OBAMA ISSUES EXECUTIVE ORDER ON INFORMATION SHARING

President Obama issued an executive order to foster sharing of cyberthreat information among the private and public sectors, highlighting the importance of this aspect of cybersecurity defense.

On February 13, following remarks given at the White House Summit on Cybersecurity and Consumer Protection held at Stanford University, President Barack Obama issued an executive order designed to promote cybersecurity information sharing within the private sector, and between the private sector and the federal government.[13] This executive order builds on a February 2013 executive order that addressed increased cybersecurity information sharing between the federal government and critical infrastructure,[14] and, together with the establishment of the Cyber Threat Intelligence Integration Center (discussed above), demonstrates the administration's focus on information sharing as a means of combating cyber threats.

The executive order directs the secretary of homeland security to encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs). ISAOs may be organized by industry, region or any other affinity, and also may be formed in response to particular cyberthreats. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations.

The secretary is directed to work with other agencies to select a nongovernmental ISAO standards organization. The standards organization will be responsible for identifying a set of voluntary standards for the creation and function of ISAOs. Those standards will be designed

---

[12]For more information on the FBI's efforts, please see our September 2014 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_September_2014.pdf.
[13]The text of the executive order may be found at http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
[14]The text of the February 2013 executive order may be found at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

to facilitate information sharing both with and among ISAOs, including through the development and adoption of automated mechanisms for the sharing of information.

The executive order directs the National Cybersecurity and Communications Integration Center (NCCIC) to collaborate with ISAOs to share information regarding identification of cybersecurity risks and how to address them. It also designates the NCCIC as a critical infrastructure protection program under the Critical Infrastructure Information Act of 2002, and authorizes the NCCIC to enter into agreements with ISAOs to promote critical infrastructure security. Other federal entities responsible for cybersecurity and related activities that address threats to public health and safety, and national and economic security, may also participate in activities governed by such agreements.

Finally, the executive order provides that federal agencies should coordinate with respect to the activities set forth in the order to ensure the appropriate protection of privacy and civil liberties.

Return to Table of Contents

NY REPORT ON CYBERSECURITY IN INSURANCE SECTOR PROVIDES INSIGHT INTO COMMON PRACTICES

New York state's "Report on Cyber Security in the Insurance Sector" presents findings on how insurance companies prepare for cyberattacks, and offers insights into common practices.

The New York State Department of Financial Services (NYDFS) has released a report, "Report on Cyber Security in the Insurance Sector," summarizing its findings from a survey of 43 insurance companies on their cybersecurity preparedness. The goal of the survey was to "obtain a horizontal perspective of the insurance industry's efforts to prevent cyber crime, protect consumers and clients in the event of a breach, and ensure the safety and soundness of their organizations." The report provides useful insight into common practices that companies in at least one industry have adopted, and also what the NYDFS, and likely other regulators, consider key aspects of a cybersecurity program.

Those surveyed by the NYDFS included health insurance providers, property and casualty insurance providers, and life insurance providers. The survey explored the following topics: the insurer's information security framework; the use and frequency of penetration testing and results; the budget and costs associated with cybersecurity; corporate governance around cybersecurity; the frequency, nature, cost of and response to cybersecurity breaches; and the company's future plans on cybersecurity. NYDFS also met with insurers and cybersecurity experts to discuss the challenges facing the industry and reviewed enterprise risk management reports that certain insurers were statutorily required to file with NYDFS.

We highlight below some of the key findings from the report:

- **Information Security Framework.** Not surprisingly, the survey found that 98 percent of insurers have an information security framework. However, what was instructive is what the NYDFS considers the five key elements of a cybersecurity program: (1) a written information security policy, (2) security awareness, and education and training, for employees, (3) information security audits, (4) management of cyber risks, and (5) incident monitoring and reporting. Similar to the approach taken by FINRA discussed earlier in this mailing, the NYDFS' main focus was on internal processes as opposed to specific technology solutions.
- **Penetration Testing. T**he NYDFS report highlights the importance of penetration testing — the process of simulating an attack on the insurer's systems and network to identify vulnerabilities — as a key component of cybersecurity protection. The report highlights the importance of conducting such tests on a frequent basis, as results may become outdated in the face of new threats.

- **Budget and Costs.** The report provides useful insight into what firms in the industry are budgeting for information security, and how they are accounting for it. According to the survey, 88 percent of insurers' information security budgets are included within their IT departments, and no institution reported having more than 7 percent of its overall budget dedicated to information security. The report noted that 14 percent of insurers dedicate less than 1 percent of their budget to security.
- **Corporate Governance and Reporting.** The report includes an analysis of the insurers' corporate governance and reporting, highlighting the importance of this component of a company's cybersecurity preparedness. The NYDFS examined which executives participate in an organization's cybersecurity governance and what the chain of reporting looks like. Significantly, the report indicates that only 14 percent of CEOs of the surveyed companies receive monthly briefings on information security. By highlighting this fact, the NYDFS is stressing the importance of CEOs being more engaged on cybersecurity issues than in the past.
- **Enterprise Risk Management Reporting.** Under New York state law, certain insurance companies are required to file an annual enterprise risk management (ERM) report with NYDFS to identify material risks to their operations. NYDFS noted that most of the surveyed companies with an ERM obligation failed to identify or discuss cybersecurity as a standalone material risk to the insurer's operations; instead, they grouped cybersecurity risks with material operational risks. NYDFS expects cybersecurity to be discussed more prominently in future ERM reports as awareness around cybersecurity increases.
- **Information Sharing.** The report notes that institutions of all sizes can "reap benefits" from membership in information-sharing organizations, such as the Financial Services – Information Sharing and Analysis Center (FS-ISAC), at a fairly low cost. The NYDFS statement is yet one more example of the increased focus on the importance of information sharing.

NEXT STEPS

NYDFS stated that it plans to use the results of its survey as part of an effort to bolster cybersecurity at regulated insurance companies. Proposed initiatives include integrating regular, targeted assessments of cybersecurity preparedness at insurance companies as a part of NYDFS' examination process, proposing enhanced regulations requiring insurance companies to meet heightened standards for cybersecurity and exploring more stringent measures in connection with the representations and warranties that third-party vendors give to insurance companies.

PRACTICE POINTS

Although the report is limited to the insurance sector and only covers the 43 companies that were surveyed, it highlights the importance that all regulators are placing on governance, training, cybersecurity audits, vendor management and Security Incident Response Plans. As regulators increasingly encourage (or mandate) these steps from regulated entities, such practices will likely be seen as "best practices" across all industry groups.

Return to Table of Contents

WHITE HOUSE RELEASES PROGRESS REPORT ON BIG DATA

A White House progress report on big data reviews how privacy, the economy and public policy are affected by developments in big data, and asserts there should be transparency in the collection of data.

On February 5, the White House released a progress report on its study of big data. The report stems from a January 2014 announcement by the White House that it had assembled a working group, led by White House Counselor John Podesta, to conduct a comprehensive 90-day review of the ways in which privacy, the economy and public policy are impacted by developments in big data, and whether policy changes are required to address advancements

in data collection technology. The recommendations from the working group's review focused on the importance of transparency of data collection practices and ensuring that big data is not used for discriminatory purposes.

The February 5 progress report outlined the following initiatives that have been taken in the year since the review began:

- A group of bipartisan legislators, working with the White House, announced the introduction of the Student Data Privacy Act. The act seeks to ensure that data collected about students through the use of apps, smart textbooks and other educational technology is used only for educational purposes and not for commercial or marketing purposes. The legislation was introduced by U.S. Reps. Luke Messer, R-Ind., and Jared Polis, D-Colo..
- The White House Council of Economic Advisers (CEA) conducted a study into the prevalence of discriminatory, or differential, pricing — the practice of companies offering different prices to different consumers — using data collected from big data technologies. The results showed that discriminatory pricing is not yet widely used, although many companies use the data collected for targeted marketing, and some companies use the data collected to experiment with personalized pricing. According to the report, while some economic research contends that discriminatory practice can be beneficial to consumers, such as when it results in children or seniors receiving reduced prices, the CEA contends that lawmakers should be wary of discriminatory pricing, as it can lead to the proliferation of fraud and scams. The White House also announced that it will release a follow-up report in the spring, which will study the ways in which big data technologies implicate certain civil rights policies and include recommendations on how to use big data to prevent discrimination.
- The White House will release a draft legislative proposal for its Consumer Privacy Bill of Rights, which proposes to provide consumers with clear, understandable and reasonable standards regarding the ways in which their personal information is used. The legislation builds on a proposal released by the president for a national standard for consumer data breach notifications and on public comments solicited by the Department of Commerce on the implications of big data technologies.
- Acknowledging the value of privacy in the treatment of all personally identifiable information handled by the federal government, the working group recommended that Privacy Act protections be extended to non-U.S. persons. The Office of Management and Budget is implementing that recommendation.
- The White House released revised national data breach legislation, the Personal Data Notification & Protection Act, in January.[15]
- President Obama's latest State of the Union Address highlighted the Precision Medicine Initiative, which is intended to advance the understanding of the ways that big data can be used to create tailored cancer treatments. The White House emphasized that data security and patient privacy will be paramount to the initiative.

One area the White House highlighted as needing further attention is the amendment of the Electronic Communications Privacy Act, which the working group's report had recommended be updated to make the standards for digital content consistent with those for physical content. The White House noted that Congress had made little progress on such an amendment since the working group's report was issued.

---

[15]For a summary of this proposed legislation, see our January 2015 *Privacy & Cybersecurity Update*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_January_2015.pdf.

Return to Table of Contents

SENATOR MARKEY REPORT HIGHLIGHTS ISSUES OF DATA PRIVACY IN THE AUTOMOTIVE INDUSTRY

Massachusetts Sen. Edward Markey has issued a report that criticizes the automotive industry's privacy practices in relation to collecting personal information through vehicle usage.

As automobile manufacturers add networked systems that control functions like navigation and safety monitoring, concerns have arisen regarding the personal information that such systems might collect. As we reported in our November 2014 *Privacy & Cybersecurity Update*, the automotive industry undertook an initiative in this area by issuing voluntary guidelines on protecting consumer privacy. In the latest development in this area, U.S. Sen. Edward J. Markey, D-Mass., has issued a report titled "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk," sharply criticizing the industry and its privacy practices in connection with such technologies. The report is the result of inquiries that Markey made of 20 major automobile manufacturers in 2014.

The report highlights the following key findings:

- Nearly 100 percent of cars currently on the market integrate wireless technologies that could be hacked or are vulnerable to privacy breaches.
- Most manufacturers were unaware or unable to report on prior hacking incidents.
- None of the manufacturers had reliable or consistent security measures in place to prevent remote access to vehicle electronics, and many manufacturers did not seem to understand the questions posed around this issue.
- Only two manufacturers had the ability to diagnose or respond to a security breach in real time.
- Manufacturers collect significant amounts of data in connection with driving history and vehicle performance.
- Most manufacturers include technologies in cars that collect and wirelessly transmit data on driving history to data centers (including third-party centers), but have not described an effective means to secure such data.
- Manufacturers vaguely describe how they use vehicle data, saying it is to "improve the customer experience," and vary as to how long they retain such data.
- Customers are usually not explicitly aware that manufacturers are collecting their vehicle data. If they are aware, they usually cannot opt out without disabling a valuable feature, such as navigation.

While Markey acknowledged the industry's recent voluntary guidelines, he raised a need for the National Highway Traffic Safety Administration and the Federal Trade Commission to collaborate on new standards that will protect driver data, security and privacy. According to Markey, such standards should: ensure that wireless access points and data-collecting features in vehicles are protected from hacking and security breaches; use penetration testing to validate security systems; use measures that respond to hacking events in real time; ensure

Return to Table of Contents

Attorney contacts appear on the next page.

SKADDEN CONTACTS

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000