Domestic and multinational companies are increasingly focused on safeguarding personal information due largely to the potential liability and reputational damage associated with data breaches. In 2010, we published an article titled “Is Data Breach Litigation a Continuing Threat?,” after countless consumer class actions seeking damages following a data breach were dismissed for failure to establish Article III standing. But, over the last few years, there has been a resurgence in the number of these actions as many have survived early dismissal. The government has also been more aggressive. A record seven administrative proceedings and court actions were brought by the Federal Trade Commission in 2014 alleging that companies failed to provide reasonable and appropriate security for consumers’ personal information.

Companies that have been successful in mitigating their liability and avoiding significant government actions after a cyber attack are those that, among other practices, developed a comprehensive written information security plan for protecting sensitive personal information, implemented robust security measures to protect this information, and responded appropriately to the attack. This white paper provides guidance on practices that companies should consider employing to safeguard personal information and, for certain target industries, to comply with statutes, regulations, guidelines, and rules prescribing safeguard standards.
ABOUT OUR PRACTICES

CYBERSECURITY AND DATA PRIVACY

Mayer Brown’s Cybersecurity and Data Privacy practice is comprised of experienced lawyers from a range of disciplines, including regulatory, intellectual property, litigation, government, financial services regulation and enforcement, employment and business & technology sourcing. We work with leading financial service firms as well as major corporations worldwide to help them comply with data privacy and security regulatory obligations. Our work includes developing information security programs, breach response plans, notification policies, and strategies for minimizing adverse consequences that may arise from litigation or governmental actions following a breach incident. We also advise on developing practical cross-border data transfer solutions—for both affiliated company transfers and for transfers to nonaffiliated parties, such as service providers and outsourcers.

LITIGATION

Mayer Brown’s Litigation practice is the firm’s largest practice with more than 450 lawyers globally, handling dispute resolution and complex, high-stakes litigation for a variety of clients in a wide array of dispute resolution venues. We are among the largest law firms in the world and have the resources to successfully handle major legal disputes across national borders. Our Litigation practice includes antitrust & competition, commercial litigation, consumer class actions, electronic discovery & records management, employment, international arbitration, IP litigation, mass torts & product liability, professional liability, securities litigation & enforcement, Supreme Court & appellate, and white collar defense & compliance.
Part One—Financial Product and Service Providers

Big Data and Cybersecurity
Standards for Safeguarding Personal Information
ABOUT THE AUTHORS  Charles E. Harris II, a partner in Mayer Brown’s Litigation & Dispute Resolution practice, defends companies in data breach class actions and counsels clients regarding compliance with data safeguarding guidelines and creating information security programs. Lei Shen, a senior associate in Mayer Brown’s Business & Technology Sourcing practice, and certified privacy professional, focuses her practice on data privacy and security, outsourcing and information technology transactions. Rebecca M. Klein, an associate in Mayer Brown’s Litigation & Dispute Resolution practice, defends companies in a wide array of commercial matters, including data breach class actions.

The authors would like to thank the following contributors to this White Paper: Lawrence R. Hamilton; Jeffrey P. Taft; Mark A. Prinsley; and Oliver Yaros.
## Part One—Financial Product and Service Providers

**INTRODUCTION** ................................................................. 1

A. Gramm-Leach Bliley Act ...................................................... 7

B. Agency Safeguard Standards .............................................. 13
   1. FTC Safeguards Rule .................................................... 13
   2. Interagency Guidelines Establishing Information Security Standards ... 14
   3. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information ......................... 16
   4. NCUA Guidelines for Safeguarding Member Information ................. 17
   5. SEC Safeguards Procedures ........................................... 19
   6. CFTC Staff Advisory No. 14-21 ..................................... 20
   7. State Insurance Regulator’s, Safeguard Rules ......................... 22

C. State Safeguard Statutes .................................................. 27
   1. Massachusetts ............................................................ 28
   2. Nevada ................................................................. 31
   3. Washington ............................................................. 32
   4. Minnesota ................................................................ 33

D. EU Data Protection Laws .................................................. 37
   1. EU Directive 95/46/EC ................................................. 38
   2. General Data Protection Regulation ................................ 39

E. Alerts and Other Guidance ............................................... 45
   1. The Federal Financial Institutions Examination Council ................. 45
   2. OCC Alerts ............................................................ 47
   3. SEC Disclosure Guidance ........................................... 48

F. PCI-DSS and Other Standards ......................................... 53
   1. Compliance Required by Payment Card Brands ...................... 53
   2. Compliance Required by State Law .................................. 54
   3. Other Data Security Standards ....................................... 54
   4. PCI-DSS and Other Standards as the Standard of Care ............ 55

**CONCLUSION** ................................................................ 61
Introduction

The regulation of data security safeguards for financial product and service providers, like other aspects of financial regulation, is a complicated, overlapping system with different regulators. Indeed, multiple federal agencies have issued rules and guidance under the Gramm-Leach-Bliley Act (“GLBA”) establishing minimum standards that these institutions must satisfy to safeguard customers’ personal information.\(^1\)

While the various rules are generally consistent, some rules are more detailed than others and some include minimum standards that are much stricter than others. In addition to these federal guidelines, state insurance regulators have established minimum safeguards standards under the GLBA for insurance companies licensed in their respective states, and state legislators have passed statutes that establish safeguards standards for entities operating in their respective states. Moreover, other countries, such as the 28 member states of the European Union (“EU”), have established minimum data security standards that arguably apply to any entity operating in their countries.

“Given this morass of authority governing data security standards, it is a feat for a financial product and service providers—particularly one that may fall under the jurisdiction of multiple federal regulators and operates in many states or in other countries—to decide on which rules or guidelines it must comply with to avoid scrutiny from regulators and/or state attorneys general.”
Given this morass of authority governing data security standards, it is a feat for a financial product and service providers—particularly one that may fall under the jurisdiction of multiple federal regulators and operates in many states or in other countries—to decide on which rules or guidelines it must comply with to avoid scrutiny from regulators and/or state attorneys general.

Understanding this issue, this paper describes, in detail, the various safeguards standards established by federal regulators, state insurance regulators, state legislators, and the EU and provides guidance on which institutions must comply with the various standards. We also discuss certain data security threat alerts and other guidance that financial product and service providers should know about, and the Payment Card Industry Data Security Standard ("PCI-DSS") and other comprehensive data security standards.
Gramm-Leach-Bliley Act
<table>
<thead>
<tr>
<th>STANDARDS</th>
<th>TYPES OF FINANCIAL PRODUCT AND SERVICE PROVIDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTC Safeguards Rule</td>
<td>Entities significantly engaged in providing financial products or services to consumers but not regulated by one of the prudential regulators referenced below</td>
</tr>
<tr>
<td>The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information issued by the OCC, the Federal Reserve, and the FDIC.</td>
<td>National banks and federal branches and agencies of foreign banks; bank holding companies and their nonbank subsidiaries or affiliates, state-chartered banks not registered with the FDIC, and foreign branches of member banks; and state-chartered banks</td>
</tr>
<tr>
<td>NCUA Guidelines for Safeguarding Member Information</td>
<td>Federally-chartered or insured credit unions</td>
</tr>
<tr>
<td>SEC Safeguards Procedures</td>
<td>Securities exchanges, brokers, and dealers; clearing agencies; mutual funds; certain investment advisers; nationally-recognized statistical rating organizations; and other individual and organization registered with the SEC</td>
</tr>
<tr>
<td>CFTC Staff Advisory No. 14-21</td>
<td>Futures exchanges and brokers; commodity pool operators; commodity trading advisors; swap dealers; major swap participants; and swap execution facilities</td>
</tr>
<tr>
<td>State Insurance Regulators Safeguard Rules</td>
<td>Insurance companies licensed by the various states</td>
</tr>
<tr>
<td>Massachusetts, Nevada, Washington, and Minnesota Safeguard Rules</td>
<td>Generally companies that access personal information of residents of the particular state and/or that operate in that state</td>
</tr>
</tbody>
</table>
Gramm-Leach-Bliley Act

The GLBA, fully effective since July 2001, declares that it is a policy of the Congress that each “financial institution” has an affirmative and continuing obligation to “protect the security and confidentiality of [its] customers’ nonpublic personal information.”2 The definitions of three terms are key: “financial institution,” “customer,” and “nonpublic personal information.”

The GLBA defines a “financial institution” as any entity “engaging in financial activities.”3 Activities that are generally considered financial in nature under the GLBA include:

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities
- Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities
- Providing financial, investment, or economic advisory services
- Issuing or selling instruments representing interests in pools of assets
- Underwriting, dealing in or making a market in securities
- Engaging in certain merchant bank activities4

Similarly, the FTC’s Safeguards Rule, discussed below, defines a financial institution as an entity “significantly engaged” in providing financial products or services.5

A “consumer” is a person who obtains financial products or services from a financial institution primarily for “personal, family,
or household purposes,” and a “customer” is a consumer who has a “customer relationship” with the institution. Lastly, “nonpublic personal information” means personal financial information “provided by a consumer to a financial institution” that “result[s] from any transaction” or is “otherwise obtained by the financial institution.”

The GLBA further states that certain agencies shall establish appropriate standards for the financial institutions subject to their jurisdiction that (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of such records; and (iii) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. The agencies tasked with prescribing these standards are the FTC, the Federal Reserve System (“Federal Reserve”), the Office of the Comptroller of the Currency (“OCC”), the Federal Deposit Insurance Corporation (“FDIC”), the National Credit Union Administration (“NCUA”), the Securities and Exchange Commission (“SEC”), the Commodity Futures Trading Commission (“CFTC”), and state insurance authorities. These agencies are required to consult and coordinate with each other to ensure that their safeguards standards are “consistent and comparable.” The standards for each of these agencies are discussed in detail below.
Agency Safeguard Standards
Agency Safeguard Standards

FTC SAFEGUARDS RULE

The FTC’s Safeguards Rule (the “Safeguards Rule”), which, as noted above, applies to entities significantly engaged in providing financial products or services to consumers, is one of the key rules implementing the GLBA. Covered entities under the Safeguards Rule include certain banks, mortgage lenders, insurance companies, investment advisers, retailers that issue payment cards and government entities, such as universities, that offer loans. The Safeguards Rule requires that these institutions develop a comprehensive written information security program (or “WISP”) that “contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue.”

The Safeguards Rule also sets forth certain elements that an institution must enact to have an appropriate WISP. The elements include:

• Designating an employee to coordinate the WISP.
• Identifying reasonably foreseeable internal and external risks to the security of customer information and assessing the sufficiency of any safeguards in place to control these risks—at a minimum, this risk assessment should include consideration of risks in each relevant area of operations, including: (i) employee training and management; (ii) information systems, including network and software design, as well as information processing, storage,
transmission, and disposal; and (iii) detecting, preventing, and responding to attacks, intrusions, or other systems failures.17

• Implementing information safeguards to control the risks identified through risk assessment.

• Regularly testing or otherwise monitoring the effectiveness of the safeguards’ key controls, systems, and procedures.18

• Overseeing service providers by: (i) taking reasonable steps to select and retain providers that are capable of maintaining appropriate safeguards for the customer information; and (ii) requiring service providers by contract to implement and maintain such safeguards.19

• Evaluating and adjusting the WISP in light of: (i) the results of the testing and monitoring; (ii) any material changes to operations; or (iii) any other circumstances that may have a material impact on the WISP.20

“Designating an employee to coordinate the WISP.”16

• Properly disposing of customer information by taking reasonable measures to protect against unauthorized access to the information in connection with its disposal, such as the burning, pulverizing, or shredding of papers containing personal information and destroying or erasing electronic media containing consumer information.21

INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

The Interagency Guidelines Establishing Information Security Standards (the “Security Guidelines”)22 are promulgated by the OCC,23 the Federal Reserve,24 and the FDIC.25 These agencies, respectively, regulate: all national banks and federal branches and agencies of foreign banks; bank holding companies and their nonbank subsidiaries or affiliates, state-chartered banks not registered with the FDIC, and foreign branches of member banks; and state-chartered banks.
Similar to the agency authority discussed above, these guidelines require that banks implement a WISP that includes “administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities” and that is designed to ensure the security of customer information, protect against any anticipated threats to the security or integrity of the information, protect against unauthorized access to or use of this information, and ensure the proper disposal of customer information.

The Security Guidelines set forth multiple requirements for the development and implementation of the WISP. The bank must:

- Involve the board of directors in approving the bank’s written WISP and overseeing its development, implementation, and maintenance.
- Perform a risk assessment to identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure of customer information.
- Design its WISP to control the identified risks proportionate to the sensitivity of the information and the complexity and scope of the bank’s activities.
- Exercise appropriate due diligence in selecting its service providers, require them to implement “appropriate measures” to meet the objectives of the Security Guidelines, and monitor them to confirm that they have satisfied their obligations.
- Monitor and adjust the WISP, as appropriate, in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank’s own changes in business arrangements.
- Report to its board at least annually, describing “the overall status of the WISP and the bank’s compliance with the [Security] Guidelines.”

“Involve the board of directors in approving the bank’s written WISP and overseeing its development, implementation, and maintenance.”
The Security Guidelines also list a number of safeguard measures that banks should consider implementing, including (i) access controls on customer information systems; (ii) access controls at physical locations containing customer information; and (iii) encryption of electronic customer information. The bank must also train its staff to implement the security program, regularly test the key controls, systems and procedures of the WISP, and develop appropriate measures for the disposal of customer information.

INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information (the “Response Guidance”) was also issued by the OCC, the Federal Reserve, the FDIC, and the OTS. The guideline directs, among other things, that each financial institution develops a “risk-based response program” to address any incidents of unauthorized access to customer information. The response program should be “appropriate to the size and complexity of the institution and the nature and scope of its activities.” Additionally, each institution should be able to address incidents of unauthorized access to customer information maintained by its service providers, and an institution’s contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the institution’s customer information.

The Response Guidance sets out several procedures that should be in place “[a]t a minimum.” The 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 Agencies’ Suspicious Activity Report (“SAR”) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing.45

• Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.46

• Notifying customers when warranted.47

Additionally, the Response Guidance states that “[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information,48 the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused” and “[i]f the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.”49 If the institution is able to determine precisely which customers’ information has been improperly accessed, it may “limit notification to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible.”50 However, if the institution is not able to identify which specific customers’ information was accessed and “the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible,” it should notify all customers in the group.51

“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.”44

NCUA GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

The NCUA’s Guidelines for Safeguarding Member Information (the “NCUA Guidelines”), which apply to federally insured credit unions,
are, by design, substantively identical to the guidelines approved by the federal banking agencies discussed above.\textsuperscript{52} The NCUA Guidelines require member credit unions to develop and implement a WISP that, at a minimum, requires that the credit union:

- Involve its board of directors in approving the credit union’s WISP and in overseeing its development, implementation, and maintenance.
- Perform a risk assessment to (i) identify foreseeable internal and external threats that could result in unauthorized disclosure of member information or access to member information systems; (ii) assess the likelihood and potential damage of these threats; and (iii) assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.
- Design its WISP to control the identified risks, taking into account the sensitivity of the information and the complexity and scope of the credit union’s activities.
- Consider adopting the following security measures that are appropriate for the credit union: (i) access controls on member information systems; (ii) access restrictions at physical locations containing member information; (iii) encryption of electronic member information while in transit or in storage on networks or systems; (iv) procedures to ensure that member information system modifications are consistent with the credit union’s WISP; (v) dual control procedures, segregation of duties, and employee background checks; (vi) monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems; (vii) response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems; and (viii) measures to protect against loss to or damage of member information due to potential environmental hazards.
- Train staff to implement the credit union’s WISP.
- Regularly test the key controls, systems and procedures of the WISP.
- Exercise appropriate due diligence in selecting its service providers, require the service providers to sign a contract agreeing to
implement appropriate measures designed to meet the objectives of the NCUA Guidelines, and, where necessary, monitor the service providers to confirm that they have satisfied their obligations.

• Monitor, evaluate, and adjust the WISP.
• Report the status of the WISP to its board or an appropriate committee of the board at least annually.53

“Design its WISP to control the identified risks, taking into account the sensitivity of the information and the complexity and scope of the credit union’s activities.”

SEC SAFEGUARDS PROCEDURES

The SEC regulates the nation’s securities markets and the brokers and dealers involved in that market.54 The agency’s safeguard procedures under Regulation S-P require that brokers, dealers, and other professionals registered with the SEC adopt written safeguard policies and procedures that are “reasonably designed” to ensure that customer records and information are secure, to protect against threats to the security of that information, and to protect against unauthorized access to or use of the information.55 Also, the rule provides that professionals registered with the SEC that maintain consumer report information56 must properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.57 In March 2008, the SEC proposed amendments to Regulation S-P that include much more detailed safeguards standards, similar to other agencies, but the amendments have not been finalized.58

In the meantime, in April 2015, the staff of the SEC Investment Management Division Guidance released a guidance update highlighting a number of measures that registered investment companies and registered investment advisers should consider in addressing cybersecurity
In the guidance update, the SEC staff provided the following nonexclusive set of recommended security measures:

- “Conduct a periodic assessment of”: (i) the nature, sensitivity and location of information that the firm collects, processes or stores, and the technology systems it uses; (ii) internal and external cybersecurity threats; (iii) security controls and processes; (iv) the impact should the information or technology systems become compromised; and (v) the effectiveness of the governance structure for the management of cybersecurity risks.

- “Create a strategy that is designed to prevent, detect and respond to cybersecurity threats,” that may include: (i) controlling access to various systems and data through management of user credentials, authentication and authorization methods, firewalls, or perimeter defenses; (ii) data encryption; (iii) protecting against the loss of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions; and (iv) development of an incident response plan.

- “Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.”

CFTC STAFF ADVISORY NO. 14-21

The CFTC regulates the futures and options markets and their constituents. In February 2014, the CFTC Division of Swap Dealer and Intermediary Oversight issued a “Staff Advisory” setting forth best practices for complying with the Commission’s regulation on safeguarding customer information. The regulation merely states that “[e]very futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, major swap participant, and swap dealer subject to the jurisdiction of the [CFTC] must adopt policies and procedures that address ... safeguards for the protection of customer records and information.”
The Staff Advisory, which is intended to be consistent with the guidelines and regulations issued by other federal financial regulators discussed above, requires institutions under the CFTC’s authority to maintain policies and procedures to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information. To this end, the CFTC recommends that institutions:

- Implement and maintain a WISP.
- Designate a specific employee with security management oversight responsibilities, who develops strategic organizational plans for implementing the required controls, is part of or reports directly to senior management or the board of directors, and designates employee(s) to implement and regularly assess the effectiveness of the program.
- Identify, in writing, all foreseeable internal and external risks to security, confidentiality, and integrity of personal information and systems processing personal information that could result in the unauthorized disclosure or other compromise of information systems.
- Establish processes and controls to assess and mitigate such risks.
- Implement safeguards to control the identified risks and maintain a written record of such designs.
- Train staff to implement the program, and provide regular refresher training.
- Regularly test or otherwise monitor the safeguard controls, systems, and policies and procedures, and maintain written records of the effectiveness of the controls.
- At least every two years, arrange for an independent party to test and monitor the systems laid out above.
- Oversee service providers that have access to customer records and information, document, in writing, that the institution is taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards, and contractually require service providers to implement and maintain appropriate safeguards.
• Regularly evaluate and adjust the program in view of various changes.
• Design and implement policies and procedures for responding to an incident involving unauthorized access, disclosure, or use of personal information.
• Provide the board of directors with an annual assessment of the program, including updates to the program, the effectiveness of the program, and instances during the year of unauthorized access or disclosure of personal information.

“Oversee service providers that have access to customer records and information, document, in writing, that the institution is taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards, and contractually require service providers to implement and maintain appropriate safeguards.”

STATE INSURANCE REGULATORS’ SAFEGUARD RULES

Insurance regulators in over 30 states and the District of Columbia have adopted safeguard standards based on the National Association of Insurance Commissioners’ Standards for Safeguarding Customer Information Model Regulation (the ‘NAIC Model Regulation’).

The NAIC Model Regulation mandates that licensed insurance companies, agents and brokers implement a comprehensive WISP including safeguards for the protection of customer information that are appropriate to the size and complexity of the licensee and the nature and scope of its activities.62

The NAIC Model Regulation provides several examples of “actions and procedures” that insurance licensees should consider in developing and implementing a WISP. As many of the rules and guidelines discussed above, these examples include:
• Identifying foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.

• Assessing the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

• Assessing the sufficiency of policies, procedures, customer information systems, and other safeguards in place to control risks.

“Insurance regulators in over 30 states and the District of Columbia have adopted safeguard standards based on the National Association of Insurance Commissioners’ Standards for Safeguarding Customer Information Model Regulation (the ‘NAIC Model Regulation’)”

• Designing a WISP to control the identified risks, commensurate with the sensitivity of the information and the complexity and scope of the licensee’s activities.

• Training staff, as appropriate, to implement the licensee’s WISP.

• Regularly testing or otherwise regularly monitoring key controls, systems, and procedures of the WISP.

• Exercising appropriate due diligence in selecting service providers.

• Requiring service providers to implement appropriate measures to meet the objectives of the NAIC Model Regulation, and taking appropriate steps to confirm that service providers have satisfied these obligations.63

“Regularly testing or otherwise regularly monitoring key controls, systems, and procedures of the WISP.”
State Safeguard Statutes
State Safeguard Statutes

To date, only four states—Massachusetts, Nevada, Washington, and Minnesota—have enacted laws applicable to companies, such as financial product and service providers, that set forth safeguards requirements for certain types of personal information.

Of these state laws, only the Massachusetts law contains detailed minimum safeguards standards that financial product and service providers and other businesses maintaining personal information of Massachusetts citizens must comply with. In contrast, Washington and Nevada generically require that entities implement “reasonable” measures to protect personal information, and Minnesota, in effect, only prohibits companies from storing particularly sensitive payment card information for more than 48 hours. But, interestingly, both Washington and Minnesota include provisions in their statutes providing that companies shall be reimbursed by negligent actors for certain losses incurred after a data breach. Each statute is discussed at length below.

Additionally, Congress is currently considering comprehensive federal data security and breach notification legislation. The White House has also spoken out in favor of a federal data breach law and proposed its own legislative language. If passed, the legislation could preempt much of the state legislation and create a uniform standard for many of the issues discussed in this paper. The proposed legislation would require companies to have data security policies respecting the use, sale, and maintenance of personal information and would create consumer notification requirements in the event of a data breach. Enforcement would fall to the FTC and to the
state attorneys general. Several major private-sector commerce groups have been supportive of such legislation, while some consumer advocacy groups worry that a weak federal standard accompanied by a strong preemption clause could harm consumers.66 At the time of this writing, debate is ongoing, and it is unclear whether any such federal law will be enacted.

“To date, only four states—Massachusetts, Nevada, Washington, and Minnesota—have enacted laws applicable to companies, such as financial product and service providers, that set forth safeguards requirements for certain types of personal information.”

**MASSACHUSETTS**

Massachusetts is one of few states that enacted specific standards for safeguarding personal information. In particular, Title 201, section 17.00 of the Code of Massachusetts Regulations, titled Standards for the Protection of Personal Information of Residents of the Commonwealth (the “MA Regulation”),69 establishes minimum requirements for safeguarding personal information contained in both paper and electronic records. The MA Regulation applies to a company that “receives, stores, maintains, processes, or otherwise has access to personal information” of Massachusetts residents “in connection with the provision of goods or services or in connection with employment.”70 These companies must develop, implement, and maintain a comprehensive WISP containing appropriate safeguard requirements, including the following elements:

- Designating an employee or employees to maintain the program.
- Identifying reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of records containing personal information, and evaluating the effectiveness of the current safeguards for limiting the risks, including: (i) ongoing employee training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
• Developing security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises.

• Imposing disciplinary measures for violations of the written program rules.

• Barring terminated employees from accessing records containing personal information.

• Overseeing service providers by: (i) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the MA Regulation and any applicable federal regulations; and (ii) requiring that service providers, by contract, implement and maintain such appropriate security measures for personal information.

• Using reasonable restrictions upon physical access to records containing personal information and storage of these records and data in locked facilities.

• Regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information safeguards as necessary to limit risks.

• Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

• Documenting responsive actions taken in connection with any incident involving a breach of security, and conducting a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.71

In addition, the WISP must include the establishment and maintenance of a security program for the company’s computers, including any wireless system. The security program must have, at least, the following elements:
- Secure user authentication protocols, including: (i) control of user IDs and other identifiers; (ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies such as biometrics or token devices; (iii) control of data security passwords to ensure that such passwords are kept in a location or format that does not compromise the security of the data they protect; (iv) restricting access to active users and active user accounts only; and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

- Secure access control measures that (i) restrict access to records and files containing personal information to those who need such information to perform their job duties and (ii) assign unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

- Reasonable monitoring of systems for unauthorized use of or access to personal information.

- Encryption of all personal information stored on laptops or other portable devices.

- For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

- Reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions and that is set to receive the most current security updates on a regular basis.

- Education and training of employees on the proper use of the computer security system and the importance of personal information security.
The MA Regulation contains many of the safeguard standards required by the federal regulators, but it is lacking the governance requirements found in the safeguard standards promulgated by certain of the federal regulators.

NEVADA

Nevada’s safeguard statute, titled “Security of Personal Information” (the “Nevada statute”), applies to any entity, including a financial product and service providers, that “handles, collects, disseminates or otherwise deals with nonpublic personal information” of Nevada residents.72 Unlike the detailed requirements of the MA Regulation, the Nevada statute simply states that an entity maintaining records containing the personal information of Nevada residents must (i) implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure and (ii) include in any contract with a third party to whom it is providing such records a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures.73 Further, companies must “take reasonable measures to ensure the destruction” of records containing personal information of Nevada residents “when the business decides that it will no longer maintain the records.”74

The Nevada statute also sets forth additional (and different) safeguard requirements for companies doing business in Nevada that accept payment cards for goods and services and those that do not. Companies accepting payment cards must comply with the current version of PCI-DSS, which, as discussed below, contains specific requirements for encryption of personal information.75 Nevada is one of three states requiring compliance with PCI-DSS. An entity that does not accept payment cards must encrypt records containing personal information being (i) transferred “through electronic, nonvoice transmission” or (ii) moved “beyond [its] logical or physical control[],” the control of its “data storage contractor,” or, in some instances, the control of a person assuming the obligation to protect the personal information.76
Notably, the Nevada statute states that a business in compliance with PCI-DSS (or the encryption requirements discussed above) shall not be liable for damages related to a data breach unless the breach is “caused by gross negligence or intentional misconduct of the [company], its officers, employees or agents.”\textsuperscript{77} This immunity seems to bar most tort claims. No court has considered the scope of this immunity under the Nevada statute, but a party seeking to limit its reach would probably contend that the immunity applies where (i) Nevada provides the applicable law and/or (ii) personal information of Nevada residents is lost. As discussed below, compliance with PCI-DSS or other safeguard standards may ultimately represent the appropriate standard of care for negligence.

**WASHINGTON**

The Washington statute concerning the security of payment card account information (the “Washington statute”) provides a remedy for certain financial product and service providers that suffer losses due to a data breach. If a “business,” defined as an entity that processes more than six million payment card transactions annually and does business with Washington residents, fails to take “reasonable care” to safeguard account information and that failure is found to be the proximate cause of a breach, the business is liable to an institution for “reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards [.]”\textsuperscript{78} A “vendor” that sells equipment for processing account information or maintains account information (e.g., cloud provider) is also liable to financial product and service providers for the cost incurred in reissuing payment cards.\textsuperscript{79} The prevailing party in any action commenced to recover these costs is entitled to recover its reasonable attorneys’ fees and costs.\textsuperscript{80}

The Washington statute does, however, provide a safe harbor. A business or vendor is not liable to an institution if (i) account information was encrypted at the time of the breach or (ii) the business or vendor was certified compliant with the current version of PCI-DSS when the breach occurred.\textsuperscript{81} The business or vendor is considered compliant if its PCI-DSS compliance was validated by an annual security assessment within the
year prior to the breach. As with the Nevada statute, no court has addressed the scope of the safe harbor. A party looking to limit the extent of the safe harbor would likely make the same arguments discussed above, when addressing the Nevada statute.

MINNESOTA

Like the Washington statute, the Minnesota statute addressing the security of account information (the “Minnesota statute”) provides redress for certain financial product and service providers injured by a data breach. Any company conducting business in Minnesota that accepts payment cards as compensation for goods and services shall not retain “the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data” more than 48 hours after authorization of a transaction. Nor shall the entity’s service provider retain this data for more than 48 hours after authorization. The requirements are taken from PCI-DSS.

Under the Minnesota statute, if there is a data breach of a business (or its service provider) and that business has violated this law, then the business shall reimburse the institution that issued any payment cards affected by the breach for the costs of reasonable actions undertaken by the entity as a result of the breach, including:

- The cancellation or reissuance of any payment card affected by the breach.
- The closure of any account affected by the breach and any action to stop payments or block transactions with respect to the account.
- The opening or reopening of any account affected by the breach.
- Any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach.
- The notification of cardholders affected by the breach.
- Damages paid by the financial institution to cardholders injured by a breach.
EU Data Protection Laws
Multinational financial product and service providers that operate in EU member states and even those that operate outside of the EU but process personal information of EU residents should be aware of the safeguards standards in the EU.

In October 1995, the European Parliament adopted the Data Protection Directive ("Directive 95/46/EC"), requiring EU member states to, among other things, implement reasonable security measures to protect personal information. All member states have enacted data protection legislation founded on Directive 95/46/EC and have created national data protection authorities to regulate compliance with that legislation. For example, the United Kingdom adopted the Data Protection Act of 1998 (the “Data Protection Act”) and created the Information Commissioner’s Office to monitor compliance with the Data Protection Act. Rather than discuss legislation from each member state, a comprehensive discussion of Directive 95/46/EC appears below.
Of note, new EU data security legislation, the General Data Protection Regulation ("GDPR"), is currently being negotiated by the European Union institutions and is due to be passed by the European Parliament at the end of 2015 or the beginning of 2016. The new legislation is designed to unify and simplify data protection in Europe and to address globalization and developments in how companies use, share, and store data. The legislation is likely to have several significant impacts. For example, given that the GDPR will be a regulation as opposed to a directive, it will directly apply to all EU member states in a uniform fashion. Further, a “one stop shop” approach has been proposed for compliance with and enforcement of data protection requirements throughout Europe, meaning that, in most cases, organizations will be able to answer to a single data protection authority in a member state concerning its compliance with data protection laws throughout Europe as opposed to being responsible to each data protection authority in the 28 member states. The GDPR is discussed in further detail below.

EU DIRECTIVE 95/46/EC

Like the rules and guidelines discussed above, Directive 95/46/EC prescribes an obligation to assess information security measures and to implement reasonable safeguards. Particularly, Article 17 of Directive 95/46/EC provides that EU member states shall:

- Provide that companies that determine how personal information is processed (such companies are called “controllers” in Directive 95/46/EC) must implement measures to protect personal data against destruction or unauthorized disclosure or access. Those measures should ensure a level of security appropriate to the risk represented by processing and the nature of the data to be protected.
- “Provide that the controller must, where processing is carried out on his or her behalf, choose a service provider that provides sufficient guarantees that it is employing proper security measures and ensure that the service provider is complying with those measures.”
- Provide that the controller must enter into a contract with the service provider processing data stipulating that (i) the service
provider shall act only on instructions from the controller and (ii) any obligations set forth in the law of the member state governing proper data security shall also apply to the service provider.

- Make sure that the parts of the contract relating to data protection and the information security measures shall be in writing or in another equivalent form.88

Article 19 of Directive 95/46/EC provides, barring certain exceptions, that member states require controllers processing personal data in their jurisdictions to notify designated national data protection authorities and, in accordance with Article 18, the notification shall include, among other information, the measures the controller has taken to secure personal information.89 Moreover, Article 25 generally requires that member states prohibit the transfer of personal data to non-member states, unless the countries are regarded by the European Commission as providing adequate legal protection for personal data consistent with European data protection laws.90

Directive 95/46/EC does not require controllers to notify data protection authorities or affected individuals about a data breach but a number of member states, such as the Czech Republic, France, and Germany, enacted legislation that requires notification and the data protection authorities in other member states have issued guidance making it clear that controllers provide such notice as a matter of good practice. The data protection authorities in each member state have the authority to commence criminal proceedings and issue fines against those organizations that fail to comply with data protection laws. For example, in the UK, the Information Commissioner’s Office has the authority to issue fines of up to £500,000 (approximately $800,000) for violations of the Data Protection Act.

GENERAL DATA PROTECTION REGULATION

The GDPR has more detailed safeguard requirements than Directive 95/46/EC. For instance, Article 22 of the regulation requires that a controller implement appropriate measures and be able to demonstrate that the processing of personal information is performed in
compliance with the GDPR. The measures include: (i) keeping documentation of all processing operations under a controller’s responsibility, implementing appropriate data protection policies and adopting measures to implement privacy by design and default; (ii) implementing appropriate data security requirements; (iii) performing a data protection impact assessment for certain types of processing; (iv) complying with the requirements for prior authorization or prior consultation of a national data protection authority; and potentially (v) designating a data protection officer.\(^{91}\)

Various articles of the GDPR address these measures, including:

- Under Article 28, documentation of processing operations must contain, at a minimum, the name of the controller, the name of any designated data protection officer, the purposes of processing, a description of personal information, the recipients of that information, where applicable, the categories of transfers to countries where personal information is going to be transferred, a general indication of the time limits for retaining personal information, and a general description of data security measures that are effective. Service providers are also required to maintain similar levels of documentation relating to their processing and under Articles 28 and 29, both controllers and service providers must make documentation relating to their processing available to the national data protection authority upon request.\(^{92}\)

- Article 30 states that, after evaluating threats to the security of personal information, a controller and its service provider must implement appropriate measures to ensure a level of security appropriate to the identified risks and to protect personal data against accidental loss, unlawful forms of processing, and unauthorized disclosure. Further, Article 30 empowers the European Commission to adopt specific technical and organizational measures to prevent unauthorized access to and disclosure of personal data and to ensure processing operations comply with the GDPR.\(^{93}\)
• Under Article 33, where the type of data being processed “present[s] specific risks to the rights and freedoms of data subjects”—such as financial data or health information—the controller must perform an impact assessment of contemplated processing operations that contains (i) a general description of the envisaged processing operations, (ii) an assessment of the risks to the rights and freedoms of data subjects, (iii) the measures to address the risks, and (iv) safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.94

• Under Article 34, controllers must consult with the national data protection authority prior to processing personal information that the controller’s impact assessment indicates will result in a high risk in the absence of measures to be taken to mitigate that risk so that the data protection authority can consider whether such processing complies with the GDPR and prevent such processing where it does not.95 Articles 35 to 37 may require (depending on the outcome of negotiations concerning the GDPR) the controller or its service provider to designate a data protection officer who would be entitled to act in an independent manner to monitor and promote compliance with the GDPR within the relevant organization.96

• Further, depending on the severity of the breach, the GDPR will require controllers to notify affected individuals about a data breach without undue delay and to notify data protection authorities, where feasible, within 72 hours. The data protection authorities in each member state will have the authority to issue fines against organizations that fail to comply with data protection laws, potentially up to either €100m (approximately $100M) or 5% of an organization’s “worldwide turnover” (i.e., its annual global sales), whichever is greater.
Alerts and Other Guidance
Alerts and Other Guidance

As shown throughout this paper, two important requirements of a WISP are monitoring security threat alerts and properly notifying regulators if a data breach occurs. The information provided by the Federal Financial Institutions Examination Council (“FFIEC”), the OCC Alerts, and the SEC Disclosure Guidance, all of which are described below, can assist a financial institution in complying with its obligations under its WISP.

THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Federal Reserve, FDIC, NCUA, OCC, and the Consumer Financial Protection Bureau (“CFPB”) and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the FFIEC issued an IT Examination Handbook focused on information security. The FFIEC Handbook gives guidance to examiners and organizations on assessing the level of security risks to the organization and evaluating the adequacy of the organization’s risk management and is meant to serve as a supplement to the agency guidance on the GLBA discussed above. Examiners may use the Handbook when evaluating a financial institution’s risk management process, including the duties, obligations, and responsibilities of the service provider for information security and the oversight exercised by the financial institution.
The FFIEC Handbook focuses on implementing a security risk management process that identifies risks, develops and implements a security strategy, and verifies the continued adequacy of risk mitigation through monitoring and testing. It includes detailed guidance on security processes, information security risk assessment, information security strategy, security controls implementation, security monitoring, and security process monitoring and updating.

The FFIEC recently released a “Cybersecurity Assessment” with “General Observations.” The FFIEC observed that the level of inherent cybersecurity risks differs significantly across financial institutions. Further, it remarked that:

“Today’s financial institutions are critically dependent on IT to conduct business operations. 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.”

Additionally, the FFIEC recently released a “Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement.” In it, the FFIEC recommends that financial institutions of all sizes participate in the Financial Services Information Sharing and Analysis Center (“FS-ISAC”), a private nonprofit information sharing forum established by financial services industry participants in response to the federal government’s efforts to facilitate the public and private sectors’ sharing of physical and cybersecurity threat and vulnerability information.
OCC ALERTS

The OCC often issues alerts and bulletins discussing data security threats. We discuss some of the more recent alerts as examples:

• **ALERT 2012-16:** “Information Security: Distributed Denial of Service Attacks and Customer Account Fraud.”\(^{106}\) This Alert reports on recent distributed denial of service (“DDoS”) attacks directed at national banks and federal savings associations and provides guidance relating to risk management and mitigation. The Alert reiterates OCC’s expectations that banks should: (i) be prepared to provide timely and accurate communication to their customers regarding website problems, risks to customers, precautions customers can take, and alternate delivery channels that will meet customer needs; (ii) consider the recent DDoS attacks and concurrent fraud against customer accounts as part of their ongoing risk management program; (iii) incorporate information sharing with other banks and service providers into their risk mitigation strategies; (iv) report DDoS attack information to law enforcement authorities and notify their supervisory office; and (v) voluntarily file a Suspicious Activity Report if a DDoS attack affects critical information of the institution, including customer account information, or damages, disables, or otherwise affects critical systems of the bank.

• **ALERT 2011-4:** “Incident Prevention and Detection—Protecting Information Security of National Banks.”\(^{107}\) This Alert highlights the need for national banks and their technology service providers (“TSPs”) to take steps to ensure that their enterprise risk management is sufficiently robust to protect and secure the bank’s own and their customers’ information. Several recent security breaches have highlighted the need for national banks and their TSPs to perform periodic risk assessments of their WISPs with respect to the prevention and detection of security incidents. The Alert also states that it expects national banks and their TSPs to review carefully the National Security Agency’s Information Assurance
Data Security: Standards for Safeguarding Personal Information

Advisory (March 28, 2011) and the United States Computer Emergency Readiness Team’s (US-CERT) Early Warning and Indicator Notice (EWIN) 11-077-01A Update.108

• **BULLETIN 2008-16:** “Application Security.”109 The Bulletin reminds banks that application security is an important component of their WISP. All applications, whether internally developed, vendor-acquired, or contracted for, should be subject to appropriate security risk assessment and mitigation processes. Vulnerabilities in applications increase operational and reputation risk as unplanned or unknown weaknesses may compromise the confidentiality, availability, and integrity of data.

**SEC DISCLOSURE GUIDANCE**

When an institution does face a data security breach, questions may arise about if, when, and how the breach must be reported to the SEC. In 2011 the SEC’s Division of Corporation Finance issued official guidance on this topic (the “SEC Guidance”).110 While not a formal rule or regulation, this guidance provides helpful direction in deciding whether the breach is a reportable event.

Though no existing SEC disclosure requirement explicitly refers to data security risks, the SEC Guidance states that “a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents.”111 Additionally, “material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.”112

The SEC Guidance lists several disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents:113

• **RISK FACTORS.** “Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.” In evaluating whether disclosure is required, the SEC expects “registrants to
evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents.” Registrants should consider “the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption” and “the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.”

• MANAGEMENT’S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS (“MD&A”). “Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.”

• DESCRIPTION OF BUSINESS. “If one or more cyber incidents materially affect a registrant’s products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant’s ‘Description of Business.’”

• LEGAL PROCEEDINGS. “If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant may need to disclose information regarding this litigation in its ‘Legal Proceedings’ disclosure.”

• FINANCIAL STATEMENT DISCLOSURES. “Cybersecurity risks and cyber incidents may have a broad impact on a registrant’s financial statements, depending on the nature and severity of the potential or actual incident.”
PCI-DSS and Other Standards
BAFIN
FISMA
SAS 70
NIST
FISMA
BSI
SITA/IATA
BAFIN
BASEL III
PCI/DSS
ISO 9000
SOX
HIPAA
SITA/IATA
GLBA
DISA
NERC/FERC
ICO/IEC 27002
NERC/FERC
ICO/IEC 27002
PCI-DSS and Other Standards

PCI-DSS, discussed briefly above, is a set of technical and business requirements for the processing of payment card data that was developed by the Payment Card Industry Security Standards Council (the “Council”). The standard generally applies, through contract, to all organizations that store, process, or transmit cardholder information, including small merchants; however, the applicable payment card brand (e.g., VISA, American Express, Discover, JCB, or MasterCard) dictates the exact compliance requirements for each business. PCI-DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The Council is responsible for managing the security standards, while compliance with PCI-DSS is enforced by payment card brands.

Compliance with PCI-DSS is not required by federal law. However, institutions are generally required to comply with PCI-DSS if they process payment cards because compliance is mandated (i) by payment card brands through their agreements and (ii) as discussed above, by certain state laws. Also, importantly, as discussed below, plaintiffs rely upon PCI-DSS to establish a negligence standard for data security compliance in class actions following a data breach.

COMPLIANCE REQUIRED BY PAYMENT CARD BRANDS

Each payment card brand has its own PCI-DSS compliance validation program and contractually obligates participating entities to be PCI-DSS compliant. Entities subject to PCI-DSS are also required to
validate their compliance annually. Covered entities that fail to comply with PCI-DSS face fines and increases in the rates the card brands charge for each transaction. Noncompliant entities may also be denied the ability to accept payment cards. If an entity does not comply with PCI-DSS and such noncompliance results in a breach of payment card data, the affected card brand may impose a fine of up to $500,000 per incident and require payment of costs associated with the breach.\textsuperscript{114}

**COMPLIANCE REQUIRED BY STATE LAW**

As discussed in detail above, to date, three states require compliance with PCI-DSS or use it as a safe harbor—Nevada, Minnesota, and Washington. Again, the Nevada statute requires organizations conducting business in the state that collect payment card data to comply with PCI-DSS.\textsuperscript{115} In this regard, the law essentially codifies PCI-DSS. The Minnesota statute is also based on a portion of PCI-DSS, thus codifying selected PCI-DSS requirements.\textsuperscript{116} Finally, the Washington statute law provides a safe harbor for businesses that adopt PCI-DSS; a covered business can escape liability if it was certified compliant with the version of PCI-DSS in force at the time of a breach.\textsuperscript{117}

**OTHER DATA SECURITY STANDARDS**

There are many data security standards that provide general outlines as well as specific techniques for implementing data. Two more well-known standards are ones published by the National Institute of Standards and Technology (“NIST”) and the International Organization for Standardization (“ISO”). First, in February 2014, NIST released the first version of its “Framework for Improving Critical Infrastructure Cybersecurity.” This framework, created through a collaboration between private data security professionals and the government, provides a structure that organizations and regulators can use to create, assess, or improve data security programs.\textsuperscript{118} The latest ISO information security standard, “ISO/IEC 27002,” was developed and published in October 2005. ISO/IEC 27002 provides best practice recommendations on information security management to be used by
professionals who are responsible for implementing or maintaining information security management systems.\(^{119}\)

**PCI-DSS AND OTHER STANDARDS AS THE STANDARD OF CARE**

Negligence (and negligent misrepresentation) are now common claims asserted in data breach class actions.\(^{120}\) If these claims are not barred by the economic loss doctrine in a particular state, their success will often rest on whether defendants employed “reasonable” security measures to protect personal information. Indeed, many companies announce that their systems will do so. In actions involving the loss of payment card data, plaintiffs typically rely on compliance with PCI-DSS to supply the appropriate standard of care since, as mentioned above, certain banks and merchants in the card processing network are generally contractually required to comply with these standards.\(^{121}\) But identifying the applicable standards of care in industries where there is no established data security standard is much more uncertain.

Given this uncertainty, compliance with some set of comprehensive data security standards, such as PCI-DSS, NIST or ISO/IEC 27002, may be sensible, particularly when the scope and nature of the data, the threat of loss, and other relevant factors call for advanced data security measures.

Implementing an accepted security standard may also help institutions avoid scrutiny from the FTC. For instance, in *In the Matter of Superior Mortgage Corp., F.T.C.*,\(^{122}\) the company allegedly violated the Safeguards Rule by collecting “sensitive customer information in connection with the mortgage application process” and “[f]ail[ing] to implement reasonable policies and procedures to protect the security and confidentiality of the information it collect[ed].”\(^{123}\)

Under its consent order, the company was ordered to obtain an assessment and report from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within 180 days after service of the order, and biennially thereafter for 10 years after service of the order, that:
• Sets forth the specific administrative, technical, and physical safeguards that the company has implemented and maintained during the reporting period;
• Explains how such safeguards are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the nonpublic personal information collected from or about consumers;
• Explains how such safeguards meet or exceed the protections required by the Safeguards Rule; and
• Certifies that the company’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected.124

The company may not have faced this inquiry from the FTC if it has implemented an accepted data security standard.125

“Given this uncertainty, compliance with some set of comprehensive data security standards, such as PCI-DSS, NIST or ISO/IEC 27002, may be sensible, particularly when the scope and nature of the data, the threat of loss, and other relevant factors call for advanced data security measures.”
Conclusion
Conclusion

Compliance with safeguards standards will remain a relevant topic for financial product and service providers as the volume of data being collected, stored, and used by these entities continues to increase. While, as shown above, there are many safeguards standards that may apply to a particular institution, the standards often overlap and a WISP containing a single set of standards covering all required safeguards can be designed and implemented. Establishing an appropriate WISP is not an easy task though. It requires the involvement of people at all levels of the organization, including the board, senior management, internal information security professionals, and IT professionals, as well as outside legal counsel and information security professionals. This white paper has hopefully provided financial product and service providers with helpful information that can be used to evaluate or reevaluate their big data and cybersecurity.
Data Security: Standards for Safeguarding Personal Information

Endnotes

1 The term “personal information” as used in this paper means a person’s first and last name or first initial and last name in combination with any one or more of the following data elements that relate to that person: (a) social security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password.


3 Id. § 6809(3) (incorporating 12 U.S.C. § 1843(k)).


5 16 C.F.R. § 313.3(k).


7 Id. § 6809(4).

8 Id. § 6801(b).

9 Id. §§ 6804, 6805(a), (b). The Federal Reserve, OCC, FDIC, OTS, and NCUA are required to implement standards by regulations and guidelines, and the other agencies are required to implement standards by rule. Id. § 6805(b)(2).

10 Id. § 6804(a)(2).

11 Also, section 215 of the Fair and Accurate Credit Transactions Act (the “FACT Act”), 15 U.S.C. 1681w, requires that the FTC, the SEC, the CFTC, federal banking agencies and the NCUA “issue final regulations requiring any person that maintains or otherwise possesses consumer information … to properly dispose of any such information[.]” Most agencies have adopted rules for disposing of customer information in accordance with the FACT Act. See, e.g., 16 C.F.R. § 682.3 (the FTC’s Disposal Rule).


14 The terms “information security” and “data security” as used in this article are synonymous. They both refer to the process of applying security measures to protect the confidentiality, integrity, and availability of personal information, whether in paper or electronic form, whether in transit or at rest. “Cybersecurity,” on the other hand, refers only to protecting electronic information.

15 16 C.F.R. § 314.3(a).
16 Id. § 314.4(a).
17 Id. § 314.4(b).
18 Id. § 314.4(c).
19 Id. § 314.4(d).
20 Id. § 314.4(e).
21 16 C.F.R. § 682.3(a), (b)(1)-(2).

22 Because the Security Guidelines appear in multiple places in the Federal Register, quotes in this section will be cited only to the version appearing in 12 C.F.R. Part 30, App. B.

23 12 C.F.R. § 30, App. B.
24 Id. § 208, App. D-2; § 225, App. F.

25 Id. § 364. The Office of Thrift Supervision (“OTS”), which promulgated safeguard standards with the other federal prudential regulators, regulated chartered and state-chartered savings banks and savings and loan associations. In July 2011, the OTS was merged into the OCC, and certain of its responsibilities were transferred to the FDIC, the Federal Reserve, and the Consumer Financial Protection Bureau (“CFPB”), and it now ceases to exist. Id.

26 Id. at App. B.II(A).
27 Id. at II(B).
28 Id. at III(A).
29 Id. at III(B).
30 Id. at III(C).
31 Id. at III(D).
32 Id. at III(E).
33 Id. at III(F).
34 Id. at III(C).
35 Id.
37 Id. §§ 208, 225.
38 Id. § 364.
39 Id. § 568, 570.
“Sensitive customer information” means “a customer’s name, address, or telephone number, in conjunction with the customer’s social security number, driver’s license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer’s account” and “any combination of components of customer information that would allow someone to log onto or access the customer’s account, such as user name and password or password and account number.” Id. at III(A)(1).

The customer notice must be given in a “clear and conspicuous manner” and should: (i) “describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use”; (ii) “generally describe what the institution has done to protect the customers’ information from further unauthorized access”; and (iii) “remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution.” Id., III(B)(1). Other information, such as “[a]n explanation of how the customer may obtain a credit report free of charge” or “[i]nformation about the availability of the FTC’s online guidance regarding steps a consumer can take to protect against identity theft” should be included “when appropriate.” Id. III(B)(1)(a)-(e).

“Consumer report information” means “any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records. Consumer report information does not include information that does not identify individuals, such as aggregate information or blind data.” Id. § 248.30(b)(1)(ii).
57 Id. § 248.30(b)(2)(i) (footnote added).


60 Id. at 1-2

61 17 C.F.R. § 160.30.


63 Id. §§ 6-9.

64 The California Financial Privacy Law applies to financial product and service providers, but it does not contain safeguard standards.


69 201 CMR 17.00 was promulgated by the Office of Consumer Affairs and Business Regulation pursuant to Massachusetts General Laws: Chapter 93H § 2(a).

70 201 CMR 17.02; see also Id. § 17.01(2).

71 Id. § 1703.


73 Id. § 603A.210(1), (2).

74 Id. § 603A.200(1).
75 Id. § 603A.215(1)

76 Id. § 603A.215(2). The requirements of the Nevada statute do not apply to data trans-
missions over a secure, private communication channel for (1) approval or processing
of negotiable instruments, electronic fund transfers, or similar payment methods or
(2) issuance of reports regarding account closures due to fraud, substantial overdrafts,
abuse of automatic teller machines, or related information regarding a customer. Id. §
603A.215(4)(b).

77 Id. § 603A.215(3).


79 Id. §19.255.020(3)(b).

80 Id. § 19.255.020(3)(a).

81 Id. § 19.255.020(2).

82 Id. § 325E.64.

83 Id. § 325E.64(2).

84 Id.

85 See PCI SSC Data Security Standards Overview, PCI Security Standards Council,
available at https://www.pcisecuritystandards.org/security_standards/ (last visited
Sept. 18, 2015).

dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm (last visited Sept. 18,


88 Directive 95/46/EC, art. 17.

89 Id. at art. 18-19.

90 Id. at art. 25.

0212+0+DOC+XML+V0//EN (last visited Sept. 18, 2015).

92 Id.

93 Id.

94 Id.

95 Id.
96 Id.


99 Id. at 1.

100 Id. at 2.

101 Id. at 1.


103 Id. at 4.


105 Id. at 1 & n.2.


111 Id.

112 Id.

113 Id.

See supra, notes 66-71.

See supra, notes 76-79.

See supra, notes 72-75.


No. 02 3136 (filed Dec. 16, 2005).

Id., Compl. ¶ 5

Id., Consent Order ¶ III.

The Third Circuit recently released its opinion in the closely watched case of Federal Trade Commission v. Wyndham Worldwide Corp., ___ F.3d ___ (3rd Cir. 2015), holding that the FTC has the authority under the “unfairness” provision of section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, to assert claims against a company for failure to implement reasonable cybersecurity safeguards. This decision effectively confirms the FTC’s authority to bring enforcement actions against entities covered by the Safeguards Rule (and those that are not) for failing to implement appropriate data security measures.
About Mayer Brown

Mayer Brown is a global legal services provider advising clients across the Americas, Asia and Europe. Our geographic strength means we can offer local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world’s largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world’s largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the “Mayer Brown Practices”). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services.

“Mayer Brown” and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

© 2015 The Mayer Brown Practices. All rights reserved.