Financial Services and Cybersecurity: The Federal Role

Updated March 23, 2016

Congressional Research Service
https://crsreports.congress.gov
R44429

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Multiple federal and state regulators oversee companies in the financial services industry. Regulatory authority is often directed at particular functions or financial services activities rather than at particular entities or companies. It is, therefore, likely that a financial services company with multiple product lines—deposits, securities, insurance—will find that it must answer to different regulators with respect to particular aspects of its operations. Five federal agencies oversee depository institutions, two regulate securities, several agencies have discrete authority over various segments of the financial sector, and several self-regulatory organizations monitor entities in the securities business.

Federal banking regulators (the Office of the Comptroller of the Currency, the Federal Reserve, and the Federal Deposit Insurance Corporation) are required to promulgate safety and soundness standards for all federally insured depository institutions to protect the stability of the nation's banking system. Some of these standards pertain to cybersecurity issues, including information security, data breaches, and destruction or theft of business records.

The *federal securities regulators* (the Securities and Exchange Commission and the Commodity Futures Trading Commission) have asserted authority over various aspects of cybersecurity in securities markets and those who trade in them. This includes requiring publicly traded financial and nonfinancial corporations to file annual and quarterly reports that provide investors with material information, a category which could include information about cybersecurity risks or breaches.

In addition, overseeing the securities industry are certain *self-regulatory organizations*—private organizations empowered by law or regulation to create and enforce industry rules, including those covering cybersecurity. These include the Financial Industry Regulatory Authority, which protects investors and oversees stock exchanges and those who trade on them. The National Futures Association has a similar role for U.S. futures exchanges and in the retail foreign exchange market.

The *Consumer Financial Protection Bureau* issues and enforces federal consumer financial protection regulations, and it has certain consumer financial protection supervisory authority over depositories and consumer finance companies not otherwise federally regulated. The Federal Trade Commission has asserted authority over certain consumer finance operations of nonfinancial companies such as retailers and hotels.

The basic authority that the federal regulators use to establish cybersecurity standards emanates from the organic legislation that established them and delineated the scope of their authority and functions. In addition, certain other laws such as the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the Gramm-Leach-Bliley Act of 1999, and the Sarbanes-Oxley Act of 2002 include provisions affecting cybersecurity of financial services. Moreover, two executive orders address the critical role of financial services in the national economy. Complementing the laws and regulations, the regulators issue guidance under a variety of names, such as policy statements, supervision and regulatory letters, financial institution letters, bulletins, and other forms of communications.

Not all regulation (or cybersecurity regulation) is done at the federal level. State governments charter and regulate state banks and all insurance companies. State securities regulators oversee securities sold within their state, and many states have laws requiring consumer notification of financial data breaches. In addition, New York State has taken advantage of the fact that the nation's financial center, Wall Street, is located in the state to be very active in certain aspects of cybersecurity regulation. This report focuses on federal laws, regulations, and executive orders.

Contents

Tables

Contacts

Introduction

Cybersecurity is a major concern of financial services providers and their federal regulators. In many ways, it is an important extension of physical security. Providers of financial services are concerned about both physical and electronic theft of money and other assets such as intellectual property. They want to prevent the destruction of property, whether it is a building or a website. They do not want to be closed down by either a physical storm or an electronic denial-of-service attack. They want to minimize human error, whether it is someone failing to secure written documents or an employee falling victim to a phishing attack. When it comes to keeping unauthorized persons away from sensitive electronic equipment, physical security and cybersecurity often overlap.

There is a growing recognition[1] by the federal government of the importance of cybersecurity in the financial services industry, as evidenced by the inclusion of financial services in the government's list of 16 critical infrastructure sectors.[2] This report provides information on the landscape of federal laws and regulatory agencies directly regulating or establishing standards for financial services cybersecurity.[3] Because each of the applicable federal laws contains specific implementation provisions, there are varying degrees and methods of regulatory oversight of cybersecurity in the financial sector. Some laws distribute authority to issue regulations and take enforcement actions among a number of agencies; others require one agency to issue implementing regulations and distribute enforcement authority among several agencies; and finally, some laws delegate all authority for issuing regulations and administrative enforcement to a single agency.

Some agencies have authority to issue notice and comment rules; others have authority to impose requirements on the institutions that they regulate by guidance that has the same legal force as notice and comment rulemaking. The federal bank supervisory agencies, which have broad general authority to issue regulations, also issue any number of types of guidance documents under a variety of names such as policy statements, supervision and regulatory (SR) letters, financial institution letters (FIL), letters, bulletins, and other forms of communication. Many of the regulators issue informal guidance and bring adjudicatory enforcement actions on a case-by-case basis that often are interpreted as precedential signals to the regulated community as to how the agency interprets aspects of its regulatory authority.

This report also provides brief descriptions and examples of the role of state law and of private sector initiatives. Its focus is, however, on the array of federal regulators and the varying ways in which federal laws impose information technology and cybersecurity requirements on financial services providers to protect the security, confidentiality, and integrity of data assembled and maintained in their businesses.

Acronyms and abbreviations are listed in a glossary at the end of this report.

[1] In a podcast released on February 5, 2016, U.S. Commodity Futures Trading Commissioner J. Christopher Giancarlo indicated that cybersecurity risks are among the potentially most disruptive risks facing financial markets, available at http://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement020416.

[2] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive (PPD)-21 "Critical Infrastructure Security and Resilience," (February 12, 2013), available at https://www.dhs.gov/strengthening-security-and-resilience-nation%E2%80%99s-critical-infrastructure.

[3] For further information on regulatory structure, see Table 1, Federal Regulators and Who They Supervise.

Financial Services Regulation Takes Many Forms

Financial services are a critical part of any modern economy. These services include

- accepting deposits;
- making loans;
- processing payments;
- providing insurance and other financial products to spread risks;
- dealing in securities such as stocks, bonds, and derivatives; and
- offering, administrating, or advising employee benefit programs.[4]

Commercial and investment banks, stock and commodity markets, and insurance companies using various securities and commodity contracts, funds, trusts, and other financial vehicles provide these services.

Banking institutions are subject to comprehensive prudential regulation touching many aspects of their daily operations. Regulation of the financial sector is based on both form (the type of charter the entity has) and function (what the entity does). There are special and distinct institution-based regulatory regimes and regulators for depositories, securities firms, and insurance companies, as well as multiple regulations based on the services or products that a financial institution provides.[5] In addition to the traditional type of financial regulation in which various financial organizations, functions, activities, or products are subjected to regulatory controls, the federal government also treats financial services as one of 16 critical infrastructure sectors with which it has arrangements to prevent disruptions to the nation's economy and harm to its wellbeing.[6]

Distinctions are often made between commercial banking (accepting deposits and making loans to businesses and individuals) and investment banking (dealing in stocks, bonds, and related securities on the bank's account or for customers). In this report, the term "bank" will be used as a general term for depository institutions. The term will be employed to cover banks, savings associations, thrifts, and credit unions with federally insured deposits. The term will also be used to cover the companies that own or control banks or thrifts (i.e., bank holding companies, financial holding companies, and savings and loan holding companies). The term "commercial bank" will be used to refer to national banks and state-chartered banks but not savings and loans or thrifts or credit unions. When focusing on a nonbank subsidiary of a holding company, however, "bank" will not be used, but the report will indicate the type of organization in question (i.e., stock exchange, insurance company, securities firm, mortgage broker, etc.).

Currently there are four federal commercial bank regulators, two federal securities regulators, one credit union federal regulator, but no primary federal regulator of insurance companies. Although primary regulation of insurance companies is the prerogative of the states, publicly traded insurance companies must comply with various securities laws and certain insurance company

[4] This description is based on the 2012 North American Industry Classification System (NAICS) 52. For more information, see U.S. Census Bureau, *Industry Statistics Portal*, "2012 NAICS: 52—Finance and Insurance," available at https://www.census.gov/econ/isp/sampler.php?naicscode=52#.

[5] See CRS Report R43087, *Who Regulates Whom and How? An Overview of U.S. Financial Regulatory Policy for Banking and Securities Markets*, by Edward V. Murphy.

[6] U.S. Department of Homeland Security, *What is Critical Infrastructure*, available at http://www.dhs.gov/what-critical-infrastructure, and U.S. Department of Homeland Security, *Financial Services Sector*, available at http://www.dhs.gov/financial-services-sector.

subsidiaries of financial holding companies may be subjected to requirements imposed by the Board of Governors of the Federal Reserve System (the Fed).[7]

Federal Banking Regulations, Regulators, and Examinations

Prudential regulation of depositories and holding companies for safety and soundness now includes concern for cybersecurity. Prudential regulation of depository institutions and their holding companies involves virtually every aspect of their capitalization, management, operations, activities, and services, as well as periodic on-site examination and continuing supervision. It is generally based upon organic legislation that establishes each regulator to charter and supervise banks,[8] savings and loans,[9] holding companies, or credit unions.[10] These laws have been amended over time to provide regulators with authority to deal with changing issues and circumstances as they have arisen.

Office of the Comptroller of the Currency

Today, the Office of the Comptroller of the Currency (OCC) is the chartering authority and primary federal regulator of national banks and federal savings associations,[11] and it relies on general authority under organic legislation to impose cybersecurity requirements on the institutions it regulates and their service providers.[12] Congress created the OCC to charter and to oversee national banks. (States can also charter banks.) The Home Owners' Loan Act of 1933[13] established a separate depository charter for savings and loan associations. However, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010[14] (Dodd-Frank) transferred responsibility for chartering and regulating federal savings and loans to the OCC.

Federal Reserve System

The Board of Governors of the Federal Reserve System has regulatory authority over an array of financial institutions and systems, and it relies on broad authority in its organic legislation to impose cybersecurity requirements on the institutions it regulates.

---

[7] See, e.g., 12 U.S.C. §5365, authorizing the Fed to impose enhanced prudential standards on bank holding companies with assets equal to or greater than $50 billion.

[8] The National Bank Act of 1863, 12 Stat. 65, ushered in a dual banking system by authorizing federally chartered banks (i.e., national banks) to be chartered and regulated by the Office of the Comptroller of the Currency (OCC), which would co-exist with banks chartered by the individual states.

[9] The Home Owners' Loan Act of 1933 authorized the formation and regulation of federally chartered savings and loan associations, paralleling the existing system of state-chartered savings and loan associations.

[10] The Federal Credit Union Act of June 26, 1934, 48 Stat. 1216, authorized the creation of federally chartered credit unions. A 1970 amendment to the Federal Credit Union Act established an independent regulator for federally chartered credit unions, the National Credit Union Administration. P.L. 91-206, 84 Stat. 49.

[11] Title III of the Dodd-Frank Act, P.L. 111-203, §312(b)(2)(B); 12 U.S.C. §5412(b)(2)(B).

[12] 12 Stat. 665.

[13] 12 U.S.C. §§1461 et seq.

[14] P.L. 111-203.

The Federal Reserve Act of 1913[15] created the Fed, headed by a Board of Governors, and gave it regulatory authority over state-chartered banks that are members of the Federal Reserve System. In 1956, the Bank Holding Company Act[16] added regulation of bank holding companies to the Fed's responsibilities. Savings and loan holding companies were added in 2010 by the Dodd-Frank Act.[17]

The Fed is the primary regulator of

- state banks that are members of the Federal Reserve System;
- U.S. branches and agencies of foreign banks;
- international operations of U.S. banks;
- companies that own banks (bank and financial holding companies);
- securities holding companies that elect to be supervised by the Fed;
- savings and loan holding companies; and
- any firm designated as a systemically significant financial institution (SIFI) by the Financial Stability Oversight Council (FSOC).

In addition, it regulates the payment, clearing, and settlement systems designated as systemically significant by the FSOC, unless regulated by the Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC).

The Fed regulates wholesale payment systems, which are used by financial institutions to transfer large-value funds and to communicate with each other. The two primary domestic interbank payment and messaging systems are the Fedwire Funds Service (operated by the Fed) and the Clearing House Interbank Payments System (CHIPS, operated by The Clearing House Payments Company, L.L.C., which is based in New York).[18]

The Fed has oversight or supervisory responsibility over designated financial market utilities, which include systemically important private sector payment systems, securities settlement systems, central securities depositories, and central counterparties. While the Fed cooperates with the other central banks in the Group of 10 to oversee SWIFT—the Society for Worldwide Interbank Financial Telecommunication, a Brussels-based entity owned by financial organizations worldwide that provides secure international messaging among banks and other financial institutions—for the purposes of critical infrastructure protection, discussed later, SWIFT is considered a communications system, and, therefore, it is overseen for cybersecurity purposes by the Department of Homeland Security.[19]

[15] P.L. 63-43.

[16] 70 Stat. 133, 12 U.S.C. §§1841 et seq.

[17] P.L. 111-203.

[18] Federal Reserve Bank Services, *Operating Circular 5,* available at https://www.frbservices.org/regulations/operating_circulars.html, covers computer access to Federal Reserve systems by member banks; Federal Reserve Bank Services, *Operating Circular 6,* available at https://www.frbservices.org/regulations/operating_circulars.html, covers access by member banks to Fedwire.

[19] Executive Order 13618, "Assignment of National Security and Emergency Preparedness," 77 *Federal Register* 40779, July 11, 2012, abolished the National Communications System (NCS), which formerly oversaw SWIFT, and reassigned this role to the Department of Homeland Security (DHS), which was NCS's parent agency.

Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) is the primary regulator of federally insured, state-chartered banks that are not members of the Federal Reserve System and all federally insured, state-chartered thrifts and savings associations.[20] It relies on broad general authority under its organic legislation to impose cybersecurity requirements on the institutions it regulates.

The Banking Act of 1933[21] created the FDIC to insure bank deposits and to act as primary federal regulator of state-chartered banks that are not members of the Federal Reserve System. Except for a few small, state-chartered banks, all banks are required to have their deposits insured by the FDIC.

National Credit Union Administration

The National Credit Union Administration (NCUA) is the federal regulator of federal credit unions and state-chartered, federally insured credit unions. It relies on broad authority under its organic legislation to impose cybersecurity requirements on the institutions it regulates.[22] Credit unions are chartered as cooperative organizations of individuals with a common bond that accept deposits of members' savings and transaction balances in the form of share accounts, pay dividends, and offer consumer credit.[23]

The Federal Credit Union Act of 1934[24] authorized federally chartered credit unions and created the Bureau of Federal Credit Unions to oversee them. The Financial Institutions Regulatory and Interest Rate Control Act of 1978[25] replaced the bureau with the National Credit Union Administration.

Consumer Financial Protection Bureau

The Consumer Financial Protection Act of 2010 (CFP Act),[26] which is Title X of Dodd-Frank,[27] created the Consumer Financial Protection Bureau (CFPB) within the Federal Reserve System. The CFPB has rulemaking, enforcement, and supervisory powers over many consumer financial

[20] The Dodd-Frank Act of 2010 allocated responsibility for regulation of state-chartered, federally insured savings associations to the FDIC.

[21] P.L. 73-66. 48 Stat. 162. The 1933 act sought to prevent investment banking from jeopardizing the soundness of commercial banking by separating them.

[22] While the NCUA has the same examination authority over national credit unions as the federal banking regulators over the depositories they regulate, NCUA lacks similar authority to examine third-party vendors. Between March 20, 1998, and December 31, 2001, NCUA had the authority to examine third-party vendors for cybersecurity around the time of the Year 2000 concerns. See P.L. 105-164, the Examination Parity and Year 2000 Readiness for Financial Institutions Act. For more on this issue, see CRS Legal Sidebar WSLG1346, *GAO Report on Depository Institution Cybersecurity Points Out NCUA's Lack of Authority to Oversee Third-Party Technology Providers*, by M. Maureen Murphy, and U.S. Government Accountability Office, *Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*, GAO-15-509, July 2015, p. 5, available at http://gao.gov/products/GAO-15-509.

[23] For more information about credit unions, see CRS Report R43167, *Policy Issues Related to Credit Union Lending*, by Darryl E. Getter.

[24] P.L. 86-354.

[25] P.L. 95-630, Title V.

[26] P.L. 111-203, Title X. 124 Stat. 1955.

[27] P.L. 111-203 §1001.

products and services, as well as the entities that sell them.[28] It has rulemaking authority over financial consumer protection laws that have cybersecurity implications, including authority to develop identity theft guidelines under the Fair and Accurate Credit Transactions Act (FACT Act)[29] and to issue regulations under the privacy provisions of the Gramm-Leach-Bliley Act (GLBA).[30] Unlike the other bank regulators, however, it does not have authority under GLBA to promulgate administrative, technical, and physical safeguards (1) to insure the security and confidentiality of "customer" records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. The CFPB has published a Supervision and Examination Manual;[31] examinations cover the protection of personally identifiable information (PII) covered by the privacy title of GLBA[32] and the Fair Credit Reporting Act (FCRA)[33] with respect to sharing of nonpublic personal information with nonaffiliated third parties.

Under its organic legislation, the CFPB has authority to issue rules declaring certain acts or practices to be unlawful because they are unfair, deceptive, or abusive. This authority is similar to authority that the Federal Trade Commission (FTC) has used to bring enforcement actions based on cybersecurity inadequacies.[34] This authority was used on March 2, 2016, by the CFPB in a cybersecurity-related enforcement action against an online payment platform. However, the CFPB's authority with respect to unfair, deceptive, or abusive practices is confined to the CFPB's general regulatory jurisdiction.[35]

The CFPB's supervisory powers include the authority to examine larger depositories for consumer compliance. The CFPB also has authority over certain nonbanks as follows:

---

[28] For more details, see CRS In Focus IF10031, *Introduction to Financial Services: The Consumer Financial Protection Bureau (CFPB)*, by David H. Carpenter and Sean M. Hoskins, and CRS Report R42572, *The Consumer Financial Protection Bureau (CFPB): A Legal Analysis*, by David H. Carpenter.

[29] P.L. 108-159 §§114 and 216, 15 U.S.C. §1691w.

[30] P.L. 106-102, Title V.

[31] CFPB Supervision and Examination Manual (2012), available at http://www.consumerfinance.gov/guidance/supervision/manual/#semanual. According to the CFPB, this is a "guide for examiners to use in overseeing companies that provide consumer financial products and services [that] describes how the CFPB supervises and examines these providers and gives ... examiners direction on how to determine if companies are complying with consumer financial protection laws."

[32] P.L. 106-102. The privacy provisions discussed in this report are in Title V of GLBA and are codified at 15 U.S.C. §§6801, et seq. Regulations implementing the data safeguards rule are at 12 C.F.R. §390((OCC), §208 (Fed), §364 (FDIC), 16 C.F.R. §314 (FTC), 17 C.F.R. §160.30 (CFTC) and 17 C.F.R.§248 (SEC)). The safeguards provisions require financial institutions to protect customer and other information that it collects. This includes promulgating administrative, technical, and physical safeguards (1) to insure the security and confidentiality of "customer" records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any "customer."

[33] 15 U.S.C. §§1681 et seq.

[34] In the Matter of Dwolla, Inc., U.S. Consumer Financial Protection Bureau Administrative Proceeding File No. 2016-CFPB-007 (March 2, 2016). This is a consent order, pursuant to which Dwolla, Inc. (Dwolla) is to undertake a number of specified actions to improve the safety and security of its operations and to pay a civil money penalty of $100,000 to the CFPB. CFPB's enforcement action is based on findings that Dwolla misrepresented to consumers the safety and security of its network and transactions and its compliance with standards promulgated by the Payment Card Industry Security Standards Council. (These standards are discussed in a later section of this report.)

[35] For further information, see CRS Report R42572, *The Consumer Financial Protection Bureau (CFPB): A Legal Analysis*, by David H. Carpenter.

> [t]he CFPB is authorized to supervise three groups of nonbanks. First, the CFPB supervises nonbanks, regardless of size, in three specific markets—mortgage companies (such as lenders, brokers, and servicers), payday lenders, and private education lenders. Second, the CFPB may supervise "larger participants" in certain consumer financial markets. The CFPB has some discretion to determine what those markets are and what constitutes a larger participant.... Third, the CFPB may supervise a nonbank if, based on consumer complaints or other sources, the CFPB has reasonable cause to determine that the nonbank poses risks to consumers in offering its financial services or products.[36]

The CFPB views protection of customer data as part of its responsibilities and has joined with the federal banking regulators to issue a cybersecurity assessment tool for financial services firms to use.[37]

Federal Financial Institutions Examination Council: Bank Examination

The Federal Financial Institutions Examination Council (FFIEC) was created by Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978,[38] to "prescribe uniform principles for the Federal examination of financial institutions by the ... [federal bank regulators] and make recommendations to promote uniformity in the supervision of these financial institutions."

All five federal depository institution regulators are members of the FFIEC.[39] The federal agency members of the FFIEC examine institutions they supervise for safety and soundness. Included in their examinations, as discussed later, is a comprehensive review of information technology and cybersecurity.

Under the privacy title of GLBA, all of the federal banking regulators, except (as previously noted) the CFPB, have authority to promulgate administrative, technical, and physical safeguards (1) to insure the security and confidentiality of "customer" records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any "customer."[40]

Banks are subject to periodic on-site examination designed to maintain the safety and soundness of the individual institutions and of the entire banking system.[41] Although every federally insured

[36] CRS In Focus IF10031, *Introduction to Financial Services: The Consumer Financial Protection Bureau (CFPB)*, by David H. Carpenter and Sean M. Hoskins.

[37] See CRS Legal Sidebar WSLG1347, *Regulators Offer Depository Institutions a Cybersecurity Self-Assessment Tool as GAO Report Finds Issues with Regulators' Monitoring of Cybersecurity for Depository Institutions*, by M. Maureen Murphy.

[38] P.L. 95-630. 92 Stat. 3641, 3694. 12 U.S.C. §§3301-3308.

[39] There is also one state financial services regulator as a rotating member of the FFIEC. FFIEC membership changed with the merger of the Office of Thrift Supervision into the OCC and the creation of the CFPB. According to the FFIEC's website, which is available at https://www.ffiec.gov/, the current membership dates to 2006 when a member of the State Liaison Committee was added to the FFIEC's membership. The State Liaison Committee "includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS)."

[40] P.L. 106-102. The privacy provisions discussed in this report are in Title V of Gramm-Leach-Bliley Act (GLBA) and codified at 15 U.S.C. §§6801 et seq. Regulations implementing the data safeguards rule are at 12 C.F.R. §390(OCC), §208 (Fed), §364 (FDIC), 16 C.F.R §314 (FTC), and 17 C.F.R §248 (SEC).

[41] The federal bank examinations are of three types: safety and soundness, systemic risk, and consumer compliance.

bank is evaluated on the same set of six factors that measure components of an institution's financial condition and operations,[42] the degree of federal oversight of a bank varies with the size of a bank, and the variety and scope of its operations.[43]

One component of a bank examination is the information technology examination, which is based on the Interagency Guidelines Establishing Information Security Standards.[44] In addition, the federal banking agencies have issued guidance advising banks that when a bank detects a breach of security involving customer information, it must promptly notify law enforcement and its regulators.[45] Customers must be notified if a reasonable investigation determines that a breach of customer information has occurred or is reasonably likely to occur.[46] The FFIEC has issued an information technology (IT) examination handbook[47] for use by examiners of the member agencies. This handbook consists of 11 separate booklets that cover specific cybersecurity areas:

- audit,
- business continuity planning,
- development and acquisition,

[42] FDIC, "Uniform Financial Institution Rating System," available at https://www.fdic.gov/regulations/laws/rules/5000-900.html. It contains the following description of the rating system:

> Composite ratings are based on a careful evaluation of an institution's managerial, operational, financial, and compliance performance. The six key components used to assess an institution's financial condition and operations are: capital adequacy, asset quality, management capability, earnings quantity and quality, the adequacy of liquidity, and sensitivity to market risk. The rating scale ranges from 1 to 5, with a rating of 1 indicating: the strongest performance and risk management practices relative to the institution's size, complexity, and risk profile; and the level of least supervisory concern. A 5 rating indicates: the most critically deficient level of performance; inadequate risk management practices relative to the institution's size, complexity, and risk profile; and the greatest supervisory concern.

[43] For example, examiners are continuously on site at large, complex banks. Most other banks have full-scope, on-site examinations at least once every 12 months, but banks with total assets of less than $500 million that meet other criteria may be examined every 18 months. 12 U.S.C. §1820(d).

[44] The "Interagency Guidelines Establishing Information Security Standards" includes a Small Entity Guide, available on the Federal Reserve's website at http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm. This covers:

> the following types of financial institutions: National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of these entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC); member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, Edge and Agreement Act Corporations, bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (Board); state non-member banks, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (FDIC); and insured savings associations and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC).

[45] "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," Supplement A to Appendix B to Parts 30, 208, 255, and 364 of 12 C.F.R.

[46] Id.

[47] U.S. Federal Financial Institutions Examination Council, *FFIEC Information Technology Examination Handbook*, Appendix B to Parts 30, 208, 255, and 364 of 12 C.F.R., available at http://ithandbook.ffiec.gov/.

[47] Id. Each booklet has an overview of the subject matter, guidance for examiners, and an appendix listing applicable laws, regulations, and guidance.

- electronic banking,
- information security,
- management,
- operations,
- outsourcing technology services,
- retail payment systems,
- supervision of technology service providers, and
- wholesale payment systems.

Nonbank Federal Regulators

In addition to federal bank regulators, other federal regulators oversee securities, markets, government-sponsored enterprises in the secondary mortgage market, agricultural credit, and certain aspects of consumer protection.

Federal Regulators of Securities and Commodities

There are two federal regulators of securities and commodities: the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC). The SEC was created by the Securities Exchange Act of 1934;[48] the CFTC was created by the Commodity Futures Trading Commission Act of 1974.[49] The SEC oversees securities exchanges, brokers and dealers, investment advisors, and mutual funds; the CFTC regulates designated contract markets, swap execution facilities, derivatives clearing organizations, swap data repositories, swap dealers, futures commission merchants, commodity pool operators, and other intermediators.

Securities and Exchange Commission

The Securities Exchange Act of 1934[50] requires publicly traded companies to disclose material[51] financial and other information to the public, primarily by filing this information with the Commission. The securities laws

> are broadly aimed at (1) investor protection; (2) maintaining fair, orderly, and efficient markets; and (3) facilitating capital formation. They do so by providing clear rules for honest dealing among securities market participants, including antifraud provisions, and a disclosure regime that requires the various entities involved in securities markets to disclose information deemed necessary for informed investment decision making.[52]

As a consequence of its responsibilities, the SEC oversees financial disclosures of both financial and nonfinancial publicly traded companies, such as large nationwide retailers. It enforces

[48] P.L. 73-291. 48 Stat. 881.

[49] P.L. 93-463 . 88 Stat. 1389.

[50] P.L. 73-291.

[51] In brief, "material" means information that an investor or potential investor would find useful in deciding whether to buy or sell the company's stock. This is usually reported on an SEC Form 8-K. For more detail, see 17 C.F.R. §211. The precise definition and its application to specific information is a matter of some contention.

[52] CRS In Focus IF10032, *Introduction to Financial Services: The Securities and Exchange Commission (SEC)*, by Gary Shorter.

prohibitions against insider trading, accounting fraud, and providing false or misleading information about securities and the companies that issue them.

Two key SEC regulations on cybersecurity are Regulation Systems Compliance and Integrity (Regulation SCI)[53] and Regulation Privacy of Consumer Financial Information (Regulation S-P).[54] Broadly speaking, Regulation SCI requires self-regulatory organizations (SROs),[55] such as the Financial Industry Regulatory Authority (FINRA), to implement comprehensive policies and procedures for their technological systems and to notify the SEC of any problems. Regulation S-P implements the provision of the privacy title of GLBA, which requires the SEC to promulgate administrative, technical, and physical safeguards (1) to insure the security and confidentiality of "customer" records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any "customer." This regulation applies to brokers and dealers, investment companies, and investment advisers registered with the SEC.[56]

The SEC's Office of Compliance Inspections and Examinations (OCIE)[57] issues *Risk Alert*s to notify regulated entities of new emphases in their inspections and examinations. A recent alert highlighted six areas of concern: governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.[58] In 2015, the OCIE alerted the securities industry to the importance of cybersecurity by publishing its "summary observations" of examinations it had conducted on approximately 100 broker-dealers or

[53] 234 Fed. Reg. 72252 (December 5, 2014), applying to entities covered by 17 C.F.R. Parts 240, 242, and 249.

[54] 17 C.F.R. §248. This regulation "applies to brokers, dealers, and investment companies, as well as to investment advisers that are registered with the Commission. It also applies to foreign (non-resident) brokers, dealers, investment companies and investment advisers that are registered with the Commission." 17 C.F.R. §248.1(b).

[55] These other entities include certain alternative trading systems (ATSs) including so-called dark pools; plan processors, such as the national market system plan; and certain exempt clearing agencies.

[56] 17 C.F.R. §248.30. The SEC has invoked this authority in one data breach incident. U.S. Securities and Exchange Commission, *R.T. Jones Capital Equities Management, Inc.* IA-4204, September 22, 2015, available at https://www.sec.gov/litigation/admin/2015/ia-4204.pdf. Violation of Regulation S-P was the basis of an SEC cease and desist order against an investment adviser, R.T. Jones Capital Equities Management, Inc. (R. T. Jones), for failing to develop and maintain policies and procedures to safeguard PII of retirement plan clients by encryption or other means. Following a data breach affecting the PII, R.T. Jones entered into a consent agreement under which it agreed to pay a $75,000 fine, to encrypt PII, and to take other remedial steps, including the appointment of an information security manager.

[57] The role of the Office and Compliance Inspections and Examinations, as explained on its website, is as follows:

> [t]he Office of Compliance Inspections and Examinations ('OCIE') protects investors through administering the SEC's nationwide examination and inspection program. Examiners in Washington DC and in the Commission's 11 regional offices conduct examinations of the nation's registered entities, including broker-dealers, transfer agents, investment advisers, investment companies, municipal advisors, the national securities exchanges, clearing agencies, SROs such as the Financial Industry Regulatory Authority ('FINRA') and the Municipal Securities Rulemaking Board, and the Public Company Accounting Oversight Board ('PCAOB'), available at https://www.sec.gov/ocie.

[58] Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, "OCIE's 2015 Cybersecurity Examination Initiative," *National Exam Program Risk Alert*, vol. 4, no. 8, (September 15, 2015 (September 15, 2015) available at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. The growing attention that the SEC is directing at cybersecurity is discussed in an article by Daniel F. Schubert, Jonathan G. Cedarbaum, and Leah Schloss, "SEC Enforcement: The SEC's Two Primary Theories in Cybersecurity Enforcement Actions," I Cybersecurity Law Report (April 8, 2015) (hereinafter, Schuber, Cedarbaum, and Schloss), available at http://www.cslawreport.com/issue/1.

registered investment advisors for vulnerability to cyberattacks. Among OCIE's 2016 examination priorities are cybersecurity and Regulation SCI compliance.[59]

Commodity Futures Trading Commission

Under the Commodity Futures Modernization Act of 2000,[60] the CFTC is required to impose requirements on the entities that it regulates to comply with the privacy title of the Gramm-Leach-Bliley Act.[61] This includes promulgating administrative, technical, and physical safeguards (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Under CFTC regulations, "[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 Commission must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."[62] The CFTC has listed best practices that are generally consistent with regulations and guidance promulgated by the FTC, the SEC, and the banking regulators.[63]

At a discussion held for securities industry participants, CFTC Chairman Timothy Massod summarized CFTC's cybersecurity regulatory efforts as follows:

> We have incorporated cybersecurity standards into our regulations, [and] required clearing houses and exchanges to maintain system safeguards and risk management programs, to

[59] Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, *National Exam Program: Examination Priorities for 2016*, available at https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

[60] P.L. 106-554. 114 Stat. 2763.

[61] P.L. 106-102, Title V. 15 U.S.C. §§6801 et seq.

[62] 17 C.F.R. §160.30.

[63] The CFTC's best practices are as follows:

> Designate a specific employee with privacy and security management oversight.
>
> Identify, in writing, all reasonably foreseeable internal and external risks to security, confidentiality, and integrity of sensitive information.
>
> Design and implement written safeguards to control the identified risks.
>
> Train staff to implement the program.
>
> Regularly test or monitor the safeguards.
>
> At least once every two years have an independent entity test and monitor the safeguards.
>
> To the extent that third party service providers have access to sensitive information, oversee and monitor their actions.
>
> Regularly revise these programs in light of new risks, changes in technology and business processes, operations, or other circumstances.
>
> Design and implement policies and procedures for responding to unauthorized access, disclosure, or use of sensitive information
>
> Provide the Board of Directors with an annual assessment of the program.

For more detail, see U.S. Commodity Futures Trading Commission, *CFTC Staff Advisory No. 14-21*, February 26, 2014, available at http://www.cftc.gov/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

> notify us promptly of incidents, to have recovery procedures in place. And we also made this a priority in our examinations.[64]

Self-Regulatory Organizations

Certain self-regulatory organizations (SROs)—private organizations empowered by law or regulation to create and enforce industry rules—also are concerned about cybersecurity. These include FINRA, which, to protect investors, oversees stock exchanges and those who trade on them. The National Futures Association (NFA) has a similar role for U.S. futures exchanges and in the retail foreign exchange market

Financial Industry Regulatory Authority

FINRA is "an independent, not-for-profit organization authorized by Congress to protect America's investors by making sure the securities industry operates fairly and honestly ... by ... writing and enforcing rules governing the activities of more than 3,957 securities firms with approximately 643,322 brokers; examining firms for compliance with those rules; fostering market transparency; and educating investors."[65] FINRA was created by the merger of the National Association of Securities Dealers, Inc. and the regulatory arm of the New York Exchange.[66]

FINRA has published a directory of SROs.[67]

National Futures Association

Among the SROs subject to the CFTC's jurisdiction,[68] the NFA oversees those individuals and companies trading on U.S. futures exchanges and in the retail foreign exchange market. Under the general category of risk management, it considers operation risk, including computer systems.[69]

The NFA manual provides guidance for members' cybersecurity programs.

Federal Insurance Regulation

There are no federal insurance regulators with roles parallel to those of the federal banking or securities agencies. The business of insurance is subject to state regulation,[70] and when there is a

---

[64] U.S. Commodities Futures Trading Commission, *Staff Roundtable on Cybersecurity and System Safeguards Testing*, March 18, 2015, available at http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/transcript031815.pdf.

[65] FINRA, "About FINRA," available on FINRA's website at https://www.finra.org/about. "Self-regulatory organization," available at https://www.law.cornell.edu/wex/self_regulatory_organization, provides a summary of the role of the securities SROs and a history of FINRA. FINRA was created pursuant to the Securities Exchange Act of 1934, 15 U.S.C. § 78o, et seq.

[66] Securities and Exchange Commission, "Order Approving Proposed Rule Change to Amend the By-Laws of the NASD to Implement Governance and Related Changes to Accommodate the Consolidation of the Member Firm Regulatory Functions of NASD and NYSE Regulation, Inc., Exchange Act Release No. 34-56,145 ," 72 Federal Register 42169, August 1, 2007.

[67] FINRA provides a directory of SROs on its website at http://www.finra.org/industry/web-crd/sro-directory.

[68] The NFA was created pursuant to the Commodity Exchange Act, 7 U.S.C. §§1-27f, et seq. For further information, see Note, "Dodd-Frank's Failure to Address CFTC Oversight of Self -Regulatory Organization Rulemaking," 1115 Columbia L.R. 69 (2013).

[69] National Futures Association, "9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs," August 30, 2015, available at http://www.nfa.futures.org/nfamanual/NFAManual.aspx.

[70] The McCarran Ferguson Act states that "[no] act of Congress shall be construed to invalidate, impair, or supersede

data breach involving an insurance company state regulators are likely to conduct an investigation.[71] However, certain federal laws, such as the privacy title of the Gramm-Leach-Bliley Act,[72] specifically impose cybersecurity requirements on insurance providers and services. These laws are generally enforced by the state authorities.

According to CRS In Focus IF10043, *Introduction to Financial Services: Insurance Regulation*, by Baird Webel,

> Each state government has a department or other entity charged with licensing and regulating insurance companies and those individuals and companies selling insurance products. States regulate the solvency of the companies and the content of insurance products as well as the market conduct of companies. Although each state sets its own laws and regulations for insurance, the National Association of Insurance Commissioners (NAIC) acts as a coordinating body that sets national standards through model laws and regulations. Models adopted by the NAIC, however, must be enacted by the states before having legal effect. The states have also developed a coordinated system of guaranty funds, designed to protect policyholders in the event of insurer insolvency.
>
> *********
>
> The Dodd-Frank Act (P.L. 111-203) in 2010 significantly altered the overall financial regulatory structure in the United States, but it largely left the state-centered insurance regulatory structure intact. The areas where the act did affect insurance regulation include (1) enhanced systemic risk regulatory authority, including authority over insurers, was vested in the Federal Reserve and in the Financial Services Oversight Council (FSOC), a new council of regulators headed by the Treasury Secretary; (2) oversight of bank and thrift holding companies, including companies with insurance subsidiaries, was consolidated in the Federal Reserve with new capital requirements added; and (3) the creation of a new Federal Insurance Office (FIO) within the Treasury Department. The Dodd-Frank Act also included measures affecting the states' oversight of surplus lines insurance and reinsurance.[73]

any law enacted by any State for the purpose of regulating the business of insurance, or which imposes a fee or tax upon such business, unless such Act specifically relates to the business of insurance." 15 U.S.C. 1012 (b). For information on state regulation of insurance companies and current federal issues, see CRS In Focus IF10043, *Introduction to Financial Services: Insurance Regulation*, by Baird Webel, and CRS Report R44046, *Insurance Regulation: Background, Overview, and Legislation in the 114th Congress*, by Baird Webel. The website of the National Association of Insurance Commissioners (NAIC) includes information on state laws governing security breach notices, National Association of Insurance Commissioners, "Special Section: Security Breach Response HQ," available at http://www.naic.org/index_security_breach.htm.

[71] In February 2015, the NAIC launched a nationwide investigation into security at health insurer Anthem Inc. after a hacker gained access to a database containing personal information on 80 million customers. *See* the NAIC's News Release, "State Insurance Commissioners Call for Multi-State Examination of Anthem," (February 5, 2015), available at http://www.naic.org/Releases/2015_docs/state_regulators_call_for_multi-state_exam_of_anthem.htm.

[72] Title V of P.L. 106-102. 113 Stat. 1338.

[73] Available at http://www.crs.gov/search/Insurance%20regulation.

Other Regulators

Federal Trade Commission

The Federal Trade Commission Act (FTC Act) established the FTC in 1914[74] to protect consumers from deceptive or unfair business practices.[75] The FTC has used this authority to bring enforcement actions against various entities, such as hotels, for failing to protect consumer information stored on computer systems.[76]

The FTC also enforces the privacy provisions of GLBA and other consumer protection statutes. Under GLBA, FTC's authority covers "financial institutions," a term that is broadly defined to include all businesses "significantly engaged" in providing financial products or services other than those subject to primary regulation by other federal regulators (i.e., the federal banking or security regulators or state insurance authorities).[77]

The FTC has promulgated a regulation requiring "all financial institutions subject to its jurisdiction" to adopt administrative, technical, and physical standards to safeguard nonpublic customer information.[78] The FTC's authority to proceed against unfair and deceptive practices, which does not extend to banks, savings associations, or credit unions, among others,[79] has been the basis of over 50 cases that the FTC has brought against companies, some of which may be financial companies, accused of engaging in unfair or deceptive practices by failing to protect personal data.[80] After complaints that its criteria for taking action on data breaches are unclear, the FTC published a guide for businesses that offers "10 practical lessons businesses can learn from the FTC's 50+ data security settlements" and briefly discusses specific breaches and explains why the FTC did or did not take action.[81]

Federal Housing Finance Agency

The Housing and Economic Recovery Act of 2008[82] created the Federal Housing Finance Agency (FHFA) to replace the previous regulators of the three housing government-sponsored enterprises

[74] 38 Stat. 717.

[75] Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce.... " 15 U.S.C. §45.

[76] See CRS Legal Sidebar WSLG938, *The Federal Trade Commission's Regulation of Data Breaches as Unfair and Deceptive Trade Practices*, by Gina Stevens.

[77] 15 U.S.C. §6805(b).

[78] 16 C.F.R., Part 314.

[79] 15 U.S.C. 45(a).

[80] For a report on recent FTC data security enforcement actions, see U.S. Federal Trade Commission, *Federal Trade Commission 2014 Privacy and Data Security Update*, available at https://www.google.com/search?q=Federal+Trade+Commission+2014+Privacy+and+Data+Security+Update&ie=utf-8&oe=utf-8.

[81] U.S. Federal Trade Commission, *Start with Security, A Guide for Business: Lessons Learned from FTC Cases*, June 2015, available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[82] P.L. 110-289. 122 Stat. 2654.

(GSEs)[83] (i.e., Fannie Mae, Freddie Mac, and the Federal Home Loan Banks). FHFA has general safety-and-soundness regulatory authority over the three GSEs.[84]

In addition, on September 6, 2008, FHFA placed Fannie Mae and Freddie Mac in voluntary conservatorship. As conservator, FHFA assumes the authority of the boards of directors and management and has broad control and oversight over the two enterprises.[85]

FHFA has issued an Advisory Bulletin on Cyber Risk Management, applicable to Fannie Mae, Freddie Mac, and the Federal Home Loan Banks.[86] It provides seven "principles-based and technology-neutral" components for cyber risk management. Included are management participation, inclusion of overall risk management, assessment of third-party relationships, and protection of sensitive, confidential, or personally identifiable information.

Farm Credit Administration

The federal government has long[87] been interested in assuring that credit is available in rural areas.[88] The Federal Farm Loan Act of 1916[89] created what is today the Farm Credit Administration (FCA), which oversees two government-sponsored enterprises (GSEs) created by the federal government to make and to facilitate financing of agricultural loans: the Farm Credit System (FCS) and the Federal Agricultural Mortgage Corporation (Farmer Mac). The Farm Credit Act of 1971[90] consolidated and revised several farm credit provisions into a coordinated Farm Credit System, designed to extend credit to farmers and ranchers through cooperatively owned banks and credit associations. This system is administered and supervised by the Farm Credit Administration.

The other agricultural GSE, Farmer Mac, is stockholder-owned and makes a secondary market in agricultural real estate mortgages, rural housing mortgages, and rural utility cooperative loans. It was created by the Agricultural Credit Act of 1987 "to establish a secondary market for agricultural real estate and rural home mortgages." The Farm Credit System Reform Act of 1996 gave Farmer Mac further authority to purchase and pool loans and issue mortgage-backed securities with guaranteed payment of principal and interest, rather than just guarantee such securities issued by other retail lenders.[91]

The FCA has no regulation that specifically addresses cybersecurity. Having said that, the agency's 2016 Regulatory Projects Plan includes consideration of "revisions to current

[83] A government-sponsored enterprise (GSE) is chartered by Congress for a public purpose, but is owned by stockholders. Fannie Mae, Freddie Mac, and the Federal Home Loan Banks were chartered to improve access to homeownership and affordable housing.

[84] 12 U.S.C. §§4511 et seq.

[85] The boards and management of Fannie Mae and Freddie Mac continue to run the enterprises, subject to FHFA approval on major decisions. The boards and senior management in place at the time of the conservatorship were reconstituted. FHFA provides information on the Fannie Mae and Freddie Mac conservatorships on its website, available at http://www.fhfa.gov/Conservatorship.

[86] Available on the FHFA's website at http://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/AB-2014-05-Cyber-Risk-Management-Guidance.aspx.

[87] For a history of federal laws providing farm credit, see the Farm Credit Administration's webpage on "History of FCA and FCS," available at https://www.fca.gov/about/history/historyFCA_FCS.html.

[88] For further information, see CRS Report RS21977, *Agricultural Credit: Institutions and Issues*, by Jim Monke.

[89] P.L. 64-158. 39 Stat 360.

[90] 12 U.S.C. §§2001 et seq.

[91] P.L. 100-233.

information technology regulations to address information security, multifactor authentication, and cybersecurity."[92]

The FCA is required to conduct a periodic examination of the institutions of the Farm Credit System (except for federal land bank associations).[93] Cybersecurity is an inherent component of these examinations. The FCA Examination Manual includes an Information Technology component in those examinations.[94] In examining an institution's security, examiners "[d]etermine if the board and management have established and maintained effective security over the institution's facilities, systems, and media that process and store vital information for business operations.... "[95] The examination is based on the FFIEC Examination Handbook and focuses on risk management and assessment, board and management oversight, and internal controls

Selected Financial Services Data Security Laws and Implementing Regulations

Major laws that include data security provisions affecting the financial services industry include Dodd-Frank,[96] the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act of 1970, the Fair and Accurate Credit Transactions Act of 2003,[97] and the Sarbanes-Oxley Act of 2002.[98] It might be noted that there are other laws, which are not specifically directed to the financial sector or to financial products, which may have an impact on the cybersecurity requirements of any financial institution. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[99] and the Health Information Technology for Economic and Clinical Health Act of 2009 impose privacy and security standards relating to health information. Financial institutions

[92] Farm Credit Administration, "FCA Regulatory Projects Plan," available at https://www.fca.gov/law/perf_plan.html.

[93] 12 U.S.C. §2254(a).

[94] See Farm Credit Administration, "Examination Manual—Information Technology," available at http://www.fca.gov/exam/info_tech.html.

[95] Farm Credit Administration, "Security: Essential Practices for Information Technology Examination Manual IT Section (October 2007)," available at http://www.fca.gov/exam/info_tech.html. This publication states the following:

> This is accomplished by:
>
> - Risk Assessment—Evaluate the adequacy of the institution's risk assessment process for information security. Key elements of this process may include management's self-assessment of the IT environment (threats, vulnerabilities, and compensating controls).
> - Risk Management—Evaluate the risk management process used to identify, control, and mitigate security risks.
> - Board and Management Oversight—Assess the adequacy of information security oversight by examining security policies, procedures, plans, and controls. Oversight responsibilities also extend to all outsourced services and contractors.
> - Internal Controls—Evaluate the effectiveness of preventive and detective controls designed to identify material deficiencies on a timely basis. Id., at 5-1.

[96] P.L. 111-203. 124 Stat. 1376.

[97] P.L. 108-159. 117 Stat. 1952.

[98] P.L. 107-204. 116 Stat. 745.

[99] P.L. 104-191. 110 Stat. 1936. For further information on HIPAA security standards, see CRS Report R43991, *HIPAA Privacy, Security, Enforcement, and Breach Notification Standards*, by C. Stephen Redhead.

holding covered health information must comply with their requirements,[100] which include data security standards.[101]

Gramm-Leach-Bliley Act of 1999

Federal regulation of the financial sector's cybersecurity also includes laws that deal with *specific concerns.* One of these is the privacy title of GLBA, which prohibits "financial institutions" from sharing nonpublic personal information of their customers with unaffiliated third-parties. Section 501 of GLBA[102] imposes obligations on "financial institutions" to "respect the privacy of ... [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information."[103] The term "financial institution" is defined broadly.[104] Under this legislation, the federal banking and securities agencies, the FTC, and state insurance regulators[105] are charged with imposing requirements on the entities that they regulate to comply with the privacy title of GLBA. This includes promulgating administrative, technical, and physical safeguards (1) to insure the security and confidentiality of "customer" records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any "customer."[106] Each of these agencies has promulgated a safeguards rule implementing this requirement.

There are also provisions in GLBA that generally prohibit, subject to certain exceptions, financial institutions from disclosing nonpublic personal information of their customers to nonaffiliated third parties. As discussed in the previous section, these provisions prohibit anyone from obtaining customer information of a financial institution by false pretenses.[107] Authority to issue regulations under these provisions has been delegated to the CFPB; enforcement authority is shared among the federal banking regulators, the federal security regulators, the state insurance commissioners, and the CFPB, with respect to the "financial institutions" which they regulate.[108]

---

[100] Jessica M. Lewis, "HIPAA: Demystifying the Implications for Financial Institutions," *North Carolina Banking Institute Journal*, vol. 8 (2008), pp. 141-164 available at http://www.law.unc.edu/journals/ncbank/volumes/volume8/citation-8-nc-banking-inst-2004/hipaa-demystifying-the-implications-for-financial-institutions/, and NACHA, "Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules," available at https://healthcare.nacha.org/sites/healthcare.nacha.org/files/files/FI%20Compliance%20Guidelines-08102012%20Update.pdf.

[101] 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

[102] P.L. 106-102. The privacy provisions discussed in this report are in Title V of GLBA and codified at 15 U.S.C. §§6801 et seq. Regulations implementing the data safeguards rule are at 12 C.F.R. §390(OCC), §208 (Fed), §364 (FDIC), 16 C.F.R §314 (FTC), and 17 C.F.R §248 (SEC).

[103] 15 U.S.C. §6801(a).

[104] GLBA, 15 U.S.C. §6809(3)(A), defines "[f]inancial institutions" as "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act" (12 U.S.C. §1843(k)). As originally enacted, the CFTC, Farm Credit institutions, and other secondary market institutions were not included. 15 U.S.C. §§6809(3)(B)-(D). Subsequent legislation added the CFTC, 7 U.S.C. §7b-2.

[105] In response to GLBA's requirement concerning the safeguarding of customer financial information, the National Conference of State Insurance Commissioners issued "Standards for Safeguarding Customer Information: Model Regulation," available at https://www.google.com/search?q=gramm-leach-bliley+safeguards+insurance&ie=utf-8&oe=utf-8.

[106] 15 U.S.C. §6801(b).

[107] 15 U.S.C. §§6821-6823. This is subject to civil and criminal penalties.

[108] P.L. 106-102 §§504 and 505, 15 U.S.C. §§6804-6805.

The FTC enforces these provisions with respect to "any institution engaged in the business of providing, financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution on a nationwide basis."[109] This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The safeguards rule also applies to companies like credit reporting agencies and automatic teller machine (ATM) operators that receive information about the customers of other financial institutions.[110]

Sarbanes-Oxley Act of 2002

Section 404 of the Sarbanes-Oxley Act of 2002[111] requires that annual reports filed with the SEC pursuant to the Securities Exchange Act of 1934 include a management evaluation of internal controls. There is some speculation that the SEC is considering this as a means of exercising "authority over the IT [information technology] controls of publicly-traded companies."[112]

The disclosure provisions discussed here apply to corporations that are required to file reports under Sections 13(a) or 15(d) of the Securities Exchange Act of 1934.[113] This includes companies with stock traded on national exchanges, foreign and domestic private issuers, and issuers of asset-backed securities. Bank holding companies, thrift holding companies, and insured depositories are required to file similar reports with their regulators. The bank regulators and the SEC have, by regulation, given those affected the option of filing one report that meets both sets of disclosure standards, or to file two reports.

Fair and Accurate Credit Transactions Act of 2003

The Fair and Accurate Credit Transactions Act (FACT Act)[114] amended the Fair Credit Reporting Act to require regulatory agencies to develop identity theft guidelines. These "red flag" guidance and regulations outline[115] "patterns, practices, and specific forms of activity that indicate the possible existence of identity theft."[116] Pursuant to this legislation, the FTC and federal banking, credit union, and securities regulators have been required to issue regulations as well as

[109] 15 U.S.C. §6827(4)(A).

[110] U.S. Federal Trade Commission, "Standards for Safeguarding Customer Information: Final Rule," 67 *Federal Register* 36485, May 23, 2002.

[111] P.L. 107-204. 116 Stat. 745, 789. 15 U.S.C. §7262.

[112] See, e.g., "The SEC's Two Primary Theories in Cybersecurity Enforcement Actions," by Daniel F. Schubert, Jonathan G. Cedarbaum, and Leah Schlauss. Cybersecurity Law Report (April 8, 2015), available at http://www.cslawreport.com/issue/1.

[113] P.L. 73 -291.

[114] P.L. 108-159 §§114 and 216. 15 U.S.C. §1681m and 15 U.S.C. §1681w.

[115] 15 U.S.C. §1681w (a)(1).

[116] 15 U.S.C. §1681m(e)(2)(A).

regulations governing the disposal of customer information.[117] The FCA has notified farm credit institutions that it may examine them for compliance with the FTC regulations.[118]

Bank Protection Act

The Bank Protection Act[119] directs the federal bank regulators (the Fed, FDIC, and OCC) to establish minimum security standards for banks and savings associations "to discourage robberies, burglaries, and larcenies and to assist in the identification and apprehension of persons who commit such acts." It includes no mention of cybersecurity.[120]

Bank Service Company Act of 1962

The Bank Service Company Act of 1962[121] authorizes the Fed, FDIC, and OCC to regulate and examine companies that provide certain services to banks (i.e., "check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution").[122] Many small banks outsource some or all of these activities. Relying on its general powers[123] under the Federal Credit Union Act, the NCUA issued a similar regulation which requires federally insured credit unions to "develop a written security program."[124]

[117] The federal banking agencies and the FTC issued "red flags" joint final rules and guidelines on November 9, 2007, 72 Fed. Reg.63718. For information on the "red flags" rules and regulations issued by the SEC and the CFTC, which became effective on May 20, 2013, see "Identity Theft Red Flags Rule," https://www.sec.gov/info/smallbus/secg/identity-theft-red-flag-secg.htm. For information on the FTC's "red flags" rule, 16 C.F.R., Part 681, see "Fighting Identity Theft with the Red Flags Rule," https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business. The FTC's Disposal Rule became effective June 1, 2005, 69 Fed. Reg. 68,690 (November 24, 2004). The federal banking regulators issued regulations on the "Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions act of 2003" on December 28, 2004, 69 Fed. Reg. 77610. Other regulations which have been issued are: 17 C.F.R., Part 248 (SEC), and 12 C.F.R. Parts 717 and 748 (NCUA).

[118] See Farm Credit Administration Information Memorandum, "FTC Regulations to Implement Affiliate Marketing, Identity Theft Red Flags, and Address Discrepancy Provisions of the FACT Act," (December 3, 2007), available at http://ww3.fca.gov/readingrm/infomemo/Lists/InformationMemorandums/DispForm.aspx?ID=200.

[119] P.L. 90-389. 12 U.S.C. §§1881-1884.

[120] Implementing regulations (e.g., 12 C.F.R. §§ 21.1-21.4) require a security program, designation of a security officer, and annual reports to the bank's board of directors with respect to the security program which includes physical safeguards and security devices.

[121] P.L. 87-856. 12 U.S.C. §§1861-1867.

[122] P.L. 87-856 §3. 12 U.S.C. §1863.

[123] 12 U.S.C. §1766(a).

[124] 12 C.F.R. §748.0. This rule covers some aspects of cybersecurity as well as physical security. It includes a requirement that the security program have a breach notice response component and that it is designed to "[e]nsure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member."

The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009

The Health Insurance Portability and Accountability Act of 1996 (HIPAA),[125] as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH),[126] creates national standards for health care providers, health insurance plans, health care clearinghouses, and their business associates[127] to comply with privacy and security requirements for paper and electronic medical records. It requires covered entities, some of which may be providing financial services for health care providers, to provide notification through first-class mail or email to individuals affected by a data breach. It also requires covered entities to notify the Secretary of the Department of Health and Human Services of breaches affecting 500 or more individuals; smaller breaches must be reported to the Secretary annually.[128]

Executive Orders

Currently, one presidential directive and two executive orders address the critical role of financial services in the national economy.[129]

First, Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience,"[130] issued on February 12, 2013, revoked Homeland Security Presidential Directive 7 (HSPD-7).[131] It identified the current 16 critical infrastructure sectors, including financial

---

[125] P.L. 104-192. 110 Stat. 1936. According to CRS Report R43991, *HIPAA Privacy, Security, Enforcement, and Breach Notification Standards*, by C. Stephen Redhead,

> The [HIPPA] Privacy Rule does not specify the types of safeguards that need to be implemented to protect ... ["protected health information"] from misuse. That is the purpose of the companion HIPAA Security Rule, under which each of the safeguards—administrative, physician, and technical—is composed of a number of standards. The security standards are designed to be scalable to the size and complexity of the covered entity, as well as technology-neutral. They include implementing security management policies and procedures, workforce security procedures, facility access controls, and controls on access to information technology (IT) systems. Each standard consists of one or more implementation specifications (i.e., detailed instructions for implementing the standard). Covered entities have considerable discretion and flexibility in how they implement the security standards.

[126] 45 C.F.R. §160.103.

[127] Business associates are entities that create, receive, maintain, or transmit protected health information for specified claims processing and management activities.

[128] Jessica M. Lewis, "HIPAA: Demystifying the Implications for Financial Institutions," *North Carolina Banking Institute Journal*, vol. 8 (2008), pp. 141-164 available at http://www.law.unc.edu/journals/ncbank/volumes/volume8/citation-8-nc-banking-inst-2004/hipaa-demystifying-the-implications-for-financial-institutions/; and NACHA, "Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules," available at https://healthcare.nacha.org/sites/healthcare.nacha.org/files/files/FI%20Compliance%20Guidelines-08102012%20Update.pdf.

[129] HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," *Public Papers of the Presidents of the United States: George W. Bush, 2003* (Washington: GPO, 2003), pp. 1739-1745, available at http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf. This superseded Presidential Decision Directive/NSC-63 of May 22, 1998, "Critical Infrastructure Protection."

[130] Executive Order PPD-21, "Directive on Critical Infrastructure Security and Resilience," *Public Papers of the Presidents of the United States: Barack Obama, 2013*, pp. 1-12, available at http://www.gpo.gov/fdsys/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf.

[131] Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and

services, and designated the Department of the Treasury as the sector-specific agency. PPD-21 set out three "strategic imperatives" as follows:

1. refine and clarify functional relationships across the federal government to advance the national unity of effort to strengthen critical infrastructure security and resilience,
2. enable efficient information exchange by identifying baseline data and systems requirements for the federal government, and
3. implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure.

Second, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[132] was issued on February 12, 2013. It ordered the National Institute of Standards and Technology (NIST) to develop a baseline cybersecurity framework that could be voluntarily adopted by the critical infrastructure sectors, including financial services. Additionally, as a sector-specific agency, Treasury was directed to consult with the Department of Homeland Security, Office of Management and Budget, and the National Security Staff to determine if existing cybersecurity regulations should be modified considering current and projected risks.

Third, Executive Order 13681, "Improving the Security of Consumer Financial Transactions,"[133] was issued on October 17, 2014. It directed federal agencies to improve the cybersecurity of their consumer financial transactions by purchasing chip and PIN payment terminals and by issuing chip and PIN payment cards for official purchases. Chip and PIN is generally considered more secure than the chip and signature system being adopted by private sector. The additional security is effective only if both payment terminals and payment cards have PINs. Except for official government payment cards, most new payment cards issued in the United States lack PINs.

State Laws

Basic State Authority

In addition to the array of federal laws, financial institutions might be subject to state consumer protection data security laws. It is more likely that such a law will be held to apply to federally insured state-chartered banks and to other financial institutions organized under state law.[134]

Protection," *Public Papers of the Presidents of the United States: George W. Bush, 2003* (Washington GPO), pp. 1739-1745, available at http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf. This superseded Presidential Decision Directive/NSC-63 of May 22, 1998, "Critical Infrastructure Protection." It identified 10 critical infrastructure sectors (including banking and finance) and designated sector-specific agencies to collaborate with other federal agencies, state and local governments, and the private sector to conduct vulnerability assessments and to encourage risk mitigation. As the sector-specific agency for banking and finance, the Department of the Treasury coordinates technical assistance and consultation to identify vulnerabilities and mitigate incidents in the financial sector.

[132] Executive Order EO 13636, "Improving Critical Infrastructure Cybersecurity," 78 *Federal Register* 11739-11744, February 19, 2013, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. For more about this executive order, see CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

[133] Executive Order EO 13681, "Improving the Security of Consumer Financial Transactions," 79 *Federal Register* 63491-63493, October 23, 2014 available at http://www.gpo.gov/fdsys/pkg/FR-2014-10-23/pdf/2014-25439.pdf.

[134] At least 12 states have laws addressing data security. Arkansas (ARK. CODE § 4-110-104); California (CAL. CIV. CODE §1798.81.5); Connecticut (Conn. Pub. Acts No. 08-167); Florida (FLA. STAT. §§ 282.318, 501.171); Indiana (IND. CODE § 24-4.9-3-3.5); Maryland (MD. CODE ANN., COM. LAW § 14-3501); Massachusetts (201 MASS. CODE REGS. §

Moreover, state requirements are likely to apply to insurance companies and to other financial firms that are not comprehensively regulated by the federal government, including industrial loan companies,[135] payday lenders, check cashers, finance companies, and mortgage loan originators.[136] There are also state securities laws and regulation, generally covering securities not publicly traded and registration and reporting of broker-dealers and stock brokers. It is beyond the scope of this report to discuss state regulation of financial services. The Conference of State Bank Supervisors (CSBS) is a central source for information on state banking regulation.[137] The website of the North American Association of Securities Administrators is a useful source for information about state securities regulations, including registration and reporting requirements regarding broker-dealers.[138]

State Laws Requiring Consumer Notification of Data Breaches

Although there are at least two data breach bills in the 114th Congress—H.R. 2205, the Data Security Act of 2015, reported out of the Committee on Financial Services, and S. 961, the Data Security Act of 2115, referred to the Committee on Commerce, Science, and Transportation—currently, there is no federal law that requires financial institutions to notify their customers of data breaches. However, the overwhelming majority of the states have enacted laws requiring consumer notification of data breaches compromising PII.[139] According to the National Conference of State Legislatures (NCSL),[140] 47 states plus the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have data breach notification laws that in general affect financial services within the individual jurisdictions. State, commonwealth, and territorial laws define what information and how many records trigger notification requirements. Many of these laws differ in how and when consumers are to be notified.

17.00) (issued pursuant to MASS. GEN. LAWS ch. 93H); Nevada (NEV. REV. STAT. § 603A.210); Oregon (OR. REV. STAT. § 646A.622); Rhode Island (R.I. GEN. LAWS § 11-49.2); Texas (TEX. BUS. & COM. CODE § 48.102); Utah (UTAH CODE § 13-44-201). Other state laws may impose data protection requirements on information held by the state government. For example, Montana recently enacted a law requiring state agencies that maintain personal information to develop procedures to protect that data. H.B. 123, §26 (2015).

[135] An industrial loan company (ILC), sometimes called an industrial loan bank, is a state-chartered bank and regulated financial entity that can be owned by commercial firms that are not regulated by a federal banking agency. If authorized by state laws, ILCs can have branches in multiple states. Many ILCs are owned by retailers and automobile companies and concentrate on providing parent company customers with financing. In some states, ILCs can accept deposits, which can be FDIC insured.

[136] For example, Texas supervises check verification companies. U.S. Congress, House Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit, Testimony of Charles G. Cooper, Banking Commissioner, Texas Department of Banking, *Examining Regulatory Burdens on Non-Depository Financial Institutions*, 114th Cong., 1st sess., April 23, 2015, available at http://financialservices.house.gov/UploadedFiles/HHRG-114-BA15-WState-CCooper-20150423.pdf.

[137] An example of this type of information is Conference of State Bank Supervisors, *Cybersecurity 101: A Resource Guide for Bank Executives*, available at https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf.

[138] For more information on state regulation of securities, see the North American Securities Administrators Association at http://www.nasaa.org/.

[139] For further information, see CRS Report R44326, *Data Security and Breach Notification Legislation: Selected Legal Issues*, by Alissa M. Dolan.

[140] National Conference of State Legislatures, *Security Breach Notification Laws*, October 22, 2015, available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

New York State

Because Wall Street and many related financial activities are located in New York City, New York State law has notable influence over the national and international financial system. The New York State Department of Financial Services (DFS) lists of over 35 separate types of financial institutions which it regulates. Among them are banks; insurance companies; credit unions; investment companies; bank holding companies; foreign bank agencies, branches, and representative offices; trusts; mortgage brokers and mortgage bankers; licensed lenders; check cashers, charitable foundations, and service contract providers; and budget planners, money transmitters, and bail bond agents.[141] DFS has issued a number of reports on cybersecurity.[142] It has expanded its examinations in the areas of cybersecurity[143] and third-party service providers (including third-party information technology providers).[144]

DFS has announced its intention to look more closely at cybersecurity policies and procedures, including third-party service provider management, multi-factor authentication, the role of the chief information security officer, application security, cybersecurity, personnel, auditing, and notifications to DFS of cybersecurity incidents. On November 9, 2015, DFS mentioned that it is considering proposing cybersecurity regulations for financial institutions, outlined the "key regulatory proposals," and invited feedback from state and federal regulators on how "to develop a comprehensive approach to cyber security regulation in the weeks and months ahead."[145]

Payment Card Industry Data Security Standard

The Payment Card Industry's Security Standards Council, founded in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc., develops, maintains, and updates Payment Card Industry Data Security Standards (PCI DSS). According to the Council,

> [m]aintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.[146]

---

[141] New York State Department of Financial Services "Who We Supervise," available at the financial institutions regulated by New York State.

[142] For a list of cybersecurity-related DFS pronouncements, see http://search.its.ny.gov/search?q=cyber&btnG=Search&entqr=0&ud=1&sort=date%3AD%3AL%3Ad1&output=xml_no_dtd&oe=UTF-8&ie=UTF-8&client=dfs_frontend&proxystylesheet=dfs_frontend&site=dfs_collection.

[143] Benjamin M. Lawsky, Superintendent of Financial Services, "New Cyber Security Examination Process," December 10,2014, available at http://search.its.ny.gov/search?q=cyber+security&btnG=Google+Search&ud=1&sort=date%3AD%3AL%3Ad1&output=xml_no_dtd&oe=UTF-8&ie=UTF-8&client=dfs_frontend&proxystylesheet=dfs_frontend&wc=200&wc_mc=1&exclude_apps=1&site=dfs_collection.

[144] Anthony J. Albanese, Acting Superintendent of New York State Department of Financial Services, "Potential New NYDFS Cyber Security Regulation Requirements," November 9, 2015, available at http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

[145] Id. Among the "key regulatory proposals" are Cyber Security Policies and Procedures, Third-party Service Provider Management, Multi-Factor Authentication, Chief Information Officer, Application Security, Cyber Security Personnel and Intelligence, Audit, and Notice of Cyber-Security Incidents.

[146] Payment Card Industry Security Standard Council's description of "PCI Security Standards," available on its website at https://www.pcisecuritystandards.org/pci_security/. For further information, see Robert J. Pile and Kristin Ward Cleare, "Pros and Cons of the Payment Card Data Security Standard," *Law 360*, March 1, 2016.

Banks issuing credit and debit cards, merchants accepting such cards, and others processing transactions involving card payments are subject to contractual obligations to comply with PCI DSS standards addressing data security. The 2015 version of the PCI DSS Standard[147] for assessing security procedures runs 115 pages and "comprises a minimum set of requirements for protecting account data [but] does not supersede local or regional laws, government regulations, or other legal requirements."[148] Among the "high level standards" are the following:

- Do not use default passwords.
- Encrypt cardholder data when transmitted over open, public networks.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.

Independent qualified security assessors are used to assess compliance with PCI DSS in most cases. The rules are enforced by a series of contracts.

One group of contracts is between a card brand, such as MasterCard, Visa, or American Express, and the banks that issue the payment cards or process payments. Another group of contracts is between these banks and those accepting the payment cards such as retailers and hotels. Since all of these contracts are private business transactions, relatively little is known about the terms.[149] An exception to this occurs when the parties contest certain provisions in court. For example, in the litigation resulting from the Target data breach of 2013, the parties introduced some of these provisions into evidence.[150]

Conclusion

Oversight of financial services cybersecurity reflects a complex and sometimes overlapping array of state and federal laws, regulators, regulations, and guidance. Cybersecurity is a critical component of protecting the vital services to the economy provided by the financial sector. Maintaining the confidentiality, security, and integrity of the data held by financial institutions is critical to sustaining the level of trust which allows businesses and consumers to rely on the financial services industry to supply services on which they depend. In recognition of the importance of the information systems that support financial services, regulators have increasingly devoted attention to cybersecurity concerns by issuing regulations and various forms of guidance.

As discussed herein, the federal government's oversight of the financial sector includes cybersecurity and involves at least four separate types of oversight and specific encouragement of voluntary cooperation.

- Depository institutions are subjected to comprehensive prudential regulation and supervision for safety and soundness.

[147] Payment Card Industry, *Data Security Standard: Requirements and Security Assessment Procedures*, Version 3.1 ed. (2015), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.

[148] *Id.*, at 3.

[149] For some information about payment system rules, see MasterCard, *Account Data Compromise User Guide*, June 26, 2014, available at https://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf, and Visa, *Visa International Operating Regulations*, October 15, 2013, available at https://usa.visa.com/dam/VCOM/download/merchants/visa-international-operating-regulations-main.pdf.

[150] In Re Target Corporation Customer Data Security Breach Litigation, U.S. District Court, D. Minn. (14-MDL-25220PAM/JJK), available at http://www.sitelevel.com/query?crid=18c705dd&query=In+re%3A+Target.

- The federal securities regulators, who administer a regime that mandates disclosure of material information by publicly traded companies, oversee the major components of the securities industry by means of a system of self-regulation. This consists of an array of SROs, such as the national securities exchanges and securities associations registered with the SEC.[151]
- Some federal agencies are charged with specific aspects of consumer protections that apply to products of the financial services industry.
- Some federal laws, which apply broadly, require financial institutions to safeguard information.
- Both Congress, with the enactment of the Consolidated Appropriations Act of 2016,[152] and the executive branch, pursuant to a series of executive orders, are encouraging voluntary cooperation among owners and operators of critical infrastructure, including financial services providers, to implement cybersecurity practices and procedures best suited to safeguard the information that they hold which is critical to U.S. national security.

There is every indication that there will be increased attention to cybersecurity at both the federal and state levels.

Glossary

CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CHIPS	Clearing House Interbank Payments System
CSBS	Conference of State Bank Supervisors
DFS	New York State Department of Financial Services
EO	Executive Order
FACT Act	Fact and Accurate Credit Transactions Act
FDIC	Federal Deposit Insurance Corporation
Fed	Board of Governors of the Federal Reserve System
FFIEC	Federal Financial Institutions Examination Council
FHFA	Federal Housing Finance Agency
FINRA	Financial Industry Regulatory Authority
FIRIRCA	Financial Institutions Regulatory and Interest Rate Control Act of 1978
FSOC	Financial Stability Oversight Council
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act of 1999
GSE	government-sponsored enterprise
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009

[151] See U.S. Government Accountability Office (GAO), *Securities and Exchange Commission: Opportunities Exist to Improve Oversight of Self-Regulatory Organizations*, GAO-08-33, November 2007, at http://www.gao.gov/new.items/d0833.pdf.

[152] P.L. 114-113.

HSPD	Homeland Security Presidential Directive
NCSL	National Conference of State Legislatures
NCUA	National Credit Union Administration
NFA	National Futures Association
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
PCI DSS	Payment Cards Industry Data Security Standard
PII	personally identifiable information
PPD	Presidential Policy Directive
SIFI	systemically important financial institution
SRO	self-regulatory organization

Table 1. Federal Financial Regulators and Who They Supervise

Regulatory Agency	Institutions Regulated
Federal Reserve	Bank holding companies and certain subsidiaries, financial holding companies, securities holding companies, savings and loan holding companies, and any firm designated as systemically significant by the FSOC
	State banks that are members of the Federal Reserve System, U.S. branches of foreign banks, and foreign branches of U.S. banks
	Payment, clearing, and settlement systems designated as systemically significant by the FSOC, unless regulated by SEC or CFTC
Office of the Comptroller of the Currency (OCC)	National banks, federally chartered thrift institutions
Federal Deposit Insurance Corporation (FDIC)	Federally insured depository institutions, including state banks and thrifts that are not members of the Federal Reserve System
National Credit Union Administration (NCUA)	Federally chartered or insured credit unions
Securities and Exchange Commission (SEC)	Securities exchanges, brokers, and dealers; clearing agencies; mutual funds; investment advisers (including hedge funds with assets over $150 million)
	Nationally recognized statistical rating organizations
	Security-based swap (SBS) dealers, major SBS participants, and SBS execution facilities
	Corporations selling securities to the public must register and make financial disclosures

Regulatory Agency	Institutions Regulated
Commodity Futures Trading Commission (CFTC)	Futures exchanges, brokers, commodity pool operators, and commodity trading advisors
	Swap dealers, major swap participants, and swap execution facilities
Federal Housing Finance Agency (FHFA)	Fannie Mae, Freddie Mac, and the Federal Home Loan Banks
Consumer Financial Protection Bureau (CFPB)	Nonbank mortgage-related firms, private student lenders, payday lenders, and larger "consumer financial entities" to be determined by the Bureau
	Consumer businesses of banks with over $10 billion in assets
	Does not supervise insurers, SEC and CFTC registrants, auto dealers, sellers of nonfinancial goods, real estate brokers and agents, and banks with assets less than $10 billion

Source: The Congressional Research Service (CRS), with information drawn from agency websites, and financial regulatory legislation.

Table 2. Selected Laws Mentioned in the Report

Name	Short Name (if any)	Public Law Number	Comment
Bank Service Company Act of 1972		P.L. 87-856	
Banking Act of 1933	Glass-Steagall Act	P.L. 73-66	Temporarily created FDIC
Banking Act of 1935			Made FDIC permanent
Commodity Futures Trading Commission Act of 1974		P.L. 93-463	CFTC
Commodity Futures Modernization Act of 2000		P.L. 106-554	Additional powers for CFTC Appendix E of Consolidated Appropriations Act, 2001
Consumer Financial Protection Act of 2010		P.L. 111-203	CFPB, Title X of Dodd-Frank
Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010	Dodd-Frank	P.L. 111-203	
Fair and Accurate Credit Transactions Act of 2003	FACT Act	P.L. 108-159	
Fair Credit Reporting Act of 1970		P.L. 91-508	Title VI of the Federal Deposit Insurance Act Amendments
FDIC Improvement Act of 1992	FDICIA	P.L. 102-242	
Federal Credit Union Act of 1934		P.L. 86-354	Credit unions
Federal Reserve Act of 1913		P.L. 63-43	Fed
Federal Trade Commission Act of 1914	FTC Act	P.L. 63-447	FTC
Financial Institutions Regulatory and Interest Rate Control Act of 1978	FIRIRCA	P.L. 95-630	NCUA, FFIEC
Gramm-Leach-Bliley Act of 1999	GLBA	P.L. 106-102	
Health Information Technology for Economic and Clinical Health Act of 2009	HITECH	P.L. 111-5	Title XIII of Division A of the American Recovery and Reinvestment Act of 2009
Health Insurance Portability and Accountability Act of 1996	HIPAA	P.L. 104-191	
Housing and Economic Recovery Act of 2008	HERA	P.L. 110-289	FHFA

Name	Short Name (if any)	Public Law Number	Comment
Sarbanes-Oxley Act of 2002	Sarbanes-Oxley	P.L. 107-204	
Securities Exchange Act 1934		P.L. 73-291	SEC

Author Information

N. Eric Weiss
Specialist in Financial Economics

M. Maureen Murphy
Legislative Attorney

Disclaimer