Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, April 2015, vol. 20, no. 1
(*http://www.arraydev.com/commerce/jibc/*)

Cybersecurity Compliance in the Financial Sector

DEREK MOHAMMED, PhD
Associate Professor, School of Business, Saint Leo University, Saint Leo, USA
Postal Address: **33701 State Road 52, Saint Leo, FL 33574, USA**
Author's Personal/Organizational Website: **www.saintleo.edu**
Email: **derek.mohammed@saintleo.edu**
Dr. Mohammed teaches undergraduate and graduates courses in Cybersecurity at Saint Leo University in Florida. His research interest includes Information Security, Risk Management, and Security Compliance.

Abstract

The financial industry represents a vast assortment of firms, agencies and institutions with operations ranging from small community banks to massive, international corporations. Managing the financial sector in the U.S. presents a herculean task to lawmakers and regulators charges with its oversight. The management of cybersecurity takes on greater complexity in considering multinationals with global partners and operations in countries with varying levels of cybersecurity sophistication. This paper investigates laws and regulations within the financial industry applicable to cybersecurity. It analyzes both compliance and regulatory issues across the financial sector at federal and state levels. It also reviews similarities and differences among compliance environments created by financial regulations. The paper distinguishes the cybersecurity operational differences and repercussions that result from the joint requirements of the Gramm-Leach-Bliley, Sarbanes-Oxley, and Dodd-Frank Acts on both small and large institutions. Finally, this paper contrasts the values and issues created by increasing compliance requirements for the financial sector..

Keywords: **Cybersecurity; Financial regulation; Compliance environment; Gramm-Leach-Bliley Act; Sarbanes-Oxley Act; Dodd-Frank Act**

INTRODUCTION

Financial regulations provide a framework seeking to promote legal and ethical behavior within the industry. However, investigations over the last fifteen years have revealed broken regulations and poor enforcement. In each scandal's wake, lawmakers passed legislation to create new standards and enforcement mechanisms. As a key pillar in a nation's economic foundation, the U.S. relies on a stable financial industry. Financial stability determines a nation's standing on the international stage. China's emergence as an international power, for example, derives partially from its economic strength. The sheer volume of assets the financial industry manages presents a highly lucrative target for criminals. Insiders engage in fraud, deceiving investors for ill-gotten profit, and others use complex financial systems for illicit purposes such as money laundering. Also damaging is the near-constant assault from cyber criminals. In order to protect consumers and ensure transparency, U.S lawmakers have empowered several regulatory bodies with oversight authority. Still, responsibility for regulatory compliance and safeguarding financial assets remains with individual institutions. Regulations create a diverse set of compliance environments that display some similarities, yet contain differences in focus and intent. Improving cybersecurity in the financial industry requires a critical evaluation of the merits and issues of compliance present in each environment. Only then can cybersecurity policy makers recommend regulations that promote efficiency while protecting the industry and its customers.

Compliance Issues

Due to the financial sector's complex nature, compliance with federal, state and local laws provide a monumental challenge. Cybersecurity further complicates the issue. As former Federal Bureau of Investigation Cyber Division Assistant Director Gordon Snow (2011) explained, "Cyber criminals have demonstrated their ability to exploit our online financial and market systems that interface with the Internet". Since the financial sector depends heavily on information technology, regulatory compliance becomes a critical cybersecurity component. Because a large portion of assets exist on paper rather than physically, protecting asset data serves as a driving force for regulation.

Ensuring coherent and active cooperation with other financial entities serves as a key to achieving compliance. The Gramm-Leach-Bliley Act (GLBA), for example, dictates how institutions collect and share information. GLBA's provisions require strict confidentiality and security for personal information institutions collect, such as account numbers, social security numbers and credit histories. Key to understanding GLBA is that the term "financial institution" carries a broad definition. The Federal Trade Commission's (FTC) Safeguards Rule sets additional standards, requiring that organizations identify personnel to oversee a security program, design and implement a safeguards program, and select service providers able to maintain implemented safeguards. Since many of the aforementioned organizations might not possess such capabilities, these regulations present a tremendous hurdle.

Compliance issues also arise at the state level. California's Notice of Security Breach Act (NSB) bears significant ramifications for the financial industry, requiring that organizations make public notifications when negligence or a cyber-attack results in data loss. Passed in 2002 and the first of its kind, NSB led to other state and federal breach notification laws.

Yet, it stands out in its call for "notification when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" (Stevens, 2012). The implied requirement is encryption of personal identifiable information, both in transport and at rest.

Data retention regulations also pose compliance issues for financial institutions. The Electronic Fund Transfer Act, Regulation E, spells out data retention requirements for institutions that hold customer accounts or provide electronic fund transfers. ATM transfers, telephone bill payments, and preauthorized transfers to or from accounts all fall under its purview. This presents another financial sector cybersecurity compliance issue, requiring secure storage for transaction information.

Regulatory Issues

The regulatory bottom line for financial institutions lies in the legal requirement to take "reasonable steps" toward cybersecurity compliance, whether information protection, data retention, or secure network architecture. As the number and sophistication of attacks increase, oversight officials will continue to develop new regulations, exacerbating compliance environments. Regulations place the onus on individual organizations to vet third-parties when outsourcing. Contracts and service level agreements must meet regulatory requirements.

Regulations within the financial industry vary tremendously based on the financial service. Some deal only with investment products and others with credit and liquidity functions (U.S. Department of Treasury, 2010). While several financial regulatory bodies exist, a great deal of institutional self-regulation also occurs. This plays a vital role, both to ensure public trust and keep federal regulators at bay. However, drastic events, such as Enron, WorldCom, and Bernie Madoff, erode trust and drive lawmakers to pass hastily drafted regulations. Similarly, a devastating cybersecurity incident would likely precipitate similar cybersecurity regulations.

Some areas of the financial sector are regulated more heavily at the state, rather than federal level. Under the McCarran-Ferguson Act of 1945, “Congress affirmed the right of the States exclusively to regulate the insurance industry" (U.S. Department of Treasury, 2010). States rely on organizations to notify entities such as the Treasury Department and the Financial and Banking Information Infrastructure Committee (FBIIC) regarding cyber incidents.

Comprehensive regulatory enforcement presents another significant challenge. Financial operations rely on cooperation between entities across the industry. As such, comprehensive cybersecurity will require a single regulatory body with cybersecurity oversight. This would also aid in formalizing the processes of applying standards developed by the financial industry. The global economy adds an additional hurdle to this challenge. Cooperation with bodies such as the European Union would facilitate smoother navigation of the international financial landscape.

According to the Financial Services Sector Coordination Council (FSSCC), the financial industry fully supports cybersecurity legislation (Blauner, 2013).

The ultimate goal lies in developing a cybersecurity framework that supports business processes. Such a framework will require a new security mindset and changes to processes such as risk management and risk mitigation. This will produce a stronger cybersecurity framework and more efficient regulations that promote a trust between financial institutions and their clients.

SIMILARITIES OF COMPLIANCE ENVIRONMENTS

Despite the diverse U.S. financial landscape, some similarities exist between compliance environments. Regulators design these environments with the intent of securing a variety of interests, from national financial stability to protecting consumers from activities such as corporate fraud, loss of personal information, and fraud against a federally insured financial institution to obtain customer information or steal money. Laws such as GLBA and bodies such as the FTC serve these interests.

As stated earlier, the GLBA requires financial institutions to protect personal customer information from improper disclosure and security threats. Whereas the GLBA has a broader definition for financial institutions, the Federal Deposit Insurance Corporation (FDIC) only protects those institutions that are insured under its provisions. It does cover some organizations considered financial institutions under GLBA, such as payday lenders or check-cashing businesses. The Electronic Fund Transfer Act (EFTA) falls under FDIC regulation and was developed to provide a framework for establishing consumer rights, as well as liabilities and responsibilities of those that use electronic fund transfer systems, including ATMs, point of sales terminals, automated clearinghouse systems, telephone bill payments, and remote banking systems.

Although the state of California NSB was previously discussed, similar laws exist in forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands. All require institutions provide security breach notifications to anyone whose personal information has been illegally accessed (Greenberg, 2012). Alabama, Kentucky, New Mexico, and South Dakota are the only states that do not have a security breach law.

The FTC's Standards for Safeguarding Customer Information requires financial institutions to have an information security plan. This plan must cover administrative, technical, and physical safeguards to ensure the security and confidentiality of customer information. It must also protect against any anticipated vulnerabilities or threats to the security and integrity of customer information, and protect against unauthorized access of this information that could potentially harm or inconvenience a customer (Federal Trade Commission, 2002). The FTCs Bureau of Consumer Protection works for the consumer to prevent fraud, deception, and unfair business practices by enforcing Federal laws that provide consumer protection thereby enhancing consumer confidence. It also empowers consumers with information that is made available to them free of charge on how to exercise their rights and identify and prevent fraud and deception, free of change.

Other compliance environments include the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) and the Sarbanes-Oxley Act (SOX). FISMA is a comprehensive legislative framework that was designed to protect government information, operations, and assets against natural or man-made

threats (Rouse, 2013). It is part of the Electronic Government Act of 2002. FISMA puts emphasis on the need for Federal agencies to develop, document and implement a program for the entire organization to provide information security for their systems that support their operations as well as their assets. The National Institute of Standards and Technology (NIST) 800-53, Recommended Security Controls for Federal Information Systems, was originally developed to support FISMA and is the primary security controls source for Federal agencies. This is important because most financial institutions are covered by the FDIC.

The FDIC is responsible for preserving and promoting confidence to the public of U.S. financial systems by insuring at least $250,000 in deposits in banks and thrift institutions; by identifying, monitoring and addressing identified risks to the deposit insurance funds; and by limiting the effect on both the economy and the financial system when a bank or thrift institution fails. The FDIC only insures checking, savings, trust, certificates of deposits, individual retirement accounts and money market deposit accounts (Marco, 2008). With all the cybersecurity threats and concerns for financial institutions, citizens should want to make sure their money is protected by using an FDIC-insured bank.

The Sarbanes-Oxley Act (SOX) is designed to prevent corporate fraud by regular documentation and disclosure of a company's internal controls, ethics code, and audit reports that can lead to review of corporate fraud. Issuers must disclose information to the public about material changes in their financial condition or operations on an urgent basis and they must be published in easy to understand terms and, where appropriate, supported by trend and qualitative data and graphic presentations. SOX is similar to the GLBA because they both review logs to identify signs of security violations and exploitations and implement processes to quickly resolve them and retain those logs to be reviewed by auditors.

Almost all of these compliance environments require financial institutions to provide some form of clear and conspicuous information disclosure to consumers, whether in writing or electronically. Specifically, the GLBA requires that disclosure must include how institutions disclose nonpublic personal information to affiliated and nonaffiliated third parties, as well as the category of information that is disclosed. Other GLBA requirements govern disclosure of information for previous customers and protection of nonpublic, personal information (U.S. Federal Trade Commission, 2002). The FDIC must meet disclosure requirements related to information such as home mortgages, education loans, and financial data held by FDIC-insured State nonmember banks. Regulations also require notification if a security breach occurs impacting an institution's customers.

DIFFERENCES OF COMPLIANCE ENVIRONMENTS

Despite their similarities, the various regulations imposed on the financial sector create a diverse set of compliance environments. These regulations possess unique characteristics and some individual laws impact organizations within the financial sector differently. Congress passed GLBA in 1999, significantly reorganizing the financial industry. Though this paper focuses on its strong provisions regarding privacy protection, one must realize its wider context as deregulation legislation. GLBA enabled institutions, such as Bank of America, to engage in multiple areas across the financial industry, including banking, securities, and insurance (Saucer, 2009). The implications of deregulation lie outside this paper's scope, with financial experts still arguing GLBA's

role in the financial crisis at the close of the last decade. Yet, the mingling of multiple financial services under one organization certainly complicates cybersecurity since it demands cybersecurity professionals in large financial organizations understand and comply with regulations across the industry.

Though GLBA deregulated the financial industry in certain aspects, conversely it introduced strong privacy regulation, focusing heavily on protecting personal information. It distinguishes itself from other regulations by requiring organizations to differentiate between "customers" and "consumers", this difference is a prime GLBA misconception. The FTC attempts to clarify this distinction as follows. An institution's consumers merely obtain financial services, but do not establish a continuing relationship. For example, an individual who uses a bank to cash a check or utilizes an ATM does not establish a continuing relationship, regardless of how frequently that individual "consumes" the institution's services. A subset of consumers, customers establish a continuing relationship with an institution via activities such as opening accounts, obtaining lines of credit, and utilizing tax preparation services or investment advising (Federal Trade Commission, 2002).

GLBA creates different requirements for safeguarding individuals' non-public information. Afforded stronger protection, customers must receive notifications containing full disclosure of an institution's information sharing and disclosure policies upon establishment of a relationship, for example when opening a checking account (Federal Trade Commission, 2002). Institutions must also provide an opt-out notice, allowing customers to prevent the institution sharing their personal information. Consumers only receive notification, which may be in "short-form" versus a full description, before an institution shares information with a non-affiliated third party.

Case law has further defined GLBA's applicability, establishing new and different compliance environments. The auto industry heavily engages in financial operations, thereby placing it under the purview of GBLA. As the GLBA took effect in the early 2000's, auto dealerships found themselves subject to penalties established under GLBA when their information security practices proved inadequate, leaving individuals' nonpublic information unsecured (Harris, 2003). Yet, a 2005 court decision found attorneys were exempt from GLBA's privacy provisions when conducting tax planning, estate planning, and personal bankruptcy. These examples serve as edification for cybersecurity professionals, highlighting the exigent need to research GLBA privacy requirements and case law, regardless of whether an organization appears outside the financial industry.

Whereas GBLA sought to safeguard personal information in concordance with financial deregulation, SOX sought to clamp down on corporate malfeasance in the wake of financial industry scandals. Applicability stands out as a key difference in SOX, which applies only to publicly traded companies, regardless of whether U.S. law classifies them as financial institutions. Another important aspect of SOX is the climate created by scandal and how it influenced Congress to rush headlong into passing legislation. Representative Michael Oxley, the bill's namesake, admitted six years after its passage that he would have written it differently, but "everyone felt like Rome was burning" (Gingrich & Kralik, 2008). While this may appear to have little bearing on cybersecurity, professionals in the cyber field should understand that a slapdash piece of legislation will

often contain more significant unforeseen consequences than legislation that undergoes greater scrutiny.

SOX introduced significant audit and monitoring requirements for publically traded organizations. It requires organizations create complex internal control frameworks for financial reporting and requires auditors to assess the efficacy of these frameworks (Hedley & Ben-Chorin, 2011). SOX Section 404 bears the greatest significance for cybersecurity professionals. However, while Section 404 does not specifically identify information security, the reality of dependence on cyber assets for both daily operations and compliance management results in heavy scrutiny on information security controls. Furthermore, SOX Section 302 places the legal burden of certifying financial reports on CEOs and CFOs. This means scrutiny on IT departments will come directly from top-tier management.

A marked difference in the SOX compliance environment is the disparity between large corporations and small companies regarding the burden of managing compliance. In 2002, many small banks lamented that the complex requirements levied by SOX Section 404 would force sales to larger firms who could absorb the costs associated with compliance (Davenport, 2004). SOX also forced changes in community banks' audit committees, demanding greater expertise in areas outside their traditional role of accounting integrity, such as legal and regulatory compliance (Naber, 2008). Testimony before the U.S. House Committee on Small Business in 2007 from leaders such as the America's Community Bankers president (Scarborough, 2007) and CEO of the Pendleton Community Bank underscored the disproportionate burden in terms of time, money, and manpower SOX placed on small and community banks.

These firms finally saw relief in 2012 via a minor provision of the Jumpstart Our Business Startups (JOBS) Act that changed registration requirements, giving them greater flexibility in how they operate (Klitsch, 2012). Smaller banks can maintain a greater number of investors without having to go public, which incurs quarterly and annual reporting proving compliance with SOX, and costs $200,000 per bank. Though smaller firms may have greater freedom to operate, cybersecurity professionals must understand that SOX constitutes a complex regulatory framework and a particularly difficult compliance environment to navigate.

GLBA and SOX created cybersecurity requirements and considerations by proxy. Neither specifically identified information technology or information security, but they nonetheless became prime areas of scrutiny for reasons discussed above. More recent legislation has created requirements that specifically identify cybersecurity reporting. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), "mandates specific information technology requirements" (Yu, 2012). As Fitzgerald noted in late 2012, the financial industry remained hard at work attempting to digest more than 2,000 pages that comprise the act. He cites multiple industry executives as preparing for a "virtual tsunami" of regulations emanating from regulatory bodies, such as the Securities and Exchange Commission (SEC) (Fitzgerald, 2012). This compliance environment has already begun to take shape, with the SEC releasing disclosure obligation guidance in late 2011. This guidance specifically references "cybersecurity risks and cyber incidents" (SEC, 2011).

Compliance with previous legislation focused on the CEO and CFO creating policy and developing frameworks, whereas Dodd-Frank compliance seems centered on the CIO preparing IT departments for a regulatory onslaught. Yu (2012) explains that cybersecurity controls, such as data security, change management, and application integrity will play a much more significant role in companies working toward Dodd-Frank compliance. Another significant difference is treatment of smaller firms. As mentioned previously, Washington regulators seem to have finally provided relief to smaller banks struggling under the weight of SOX. However, despite initial assurances to the contrary, Dodd-Frank stands to add potentially crushing regulatory requirements on smaller firms. Industry continues to wrestle with the impacts of GLBA and SOX. Dodd-Frank represents the latest wave in the financial industry compliance environment, one that promises to change its metaphorical topography drastically

BENEFITS OF INCREASING COMPLIANCE REQUIREMENTS

The recent financial crises have prompted multiple nations, specifically the U.S., to take regulatory measures in the financial industry to avoid future economic disasters. Financial institutions play a major role in the global economy and its health can determine whether countries improve or decline. Financial institutions are used in many ways to aid businesses and citizens to operate in a fair and lawful manner. However, not all businesses or citizens utilize financial institutions for their intended purposes. Some use financial institutions to fund terrorism, run illegal money exchanges, and conduct other illegal activities that endanger global markets and people's lives. Adequate cybersecurity helps guard against these and other illicit activities.

The goal of a compliance regulation is to ensure fair and equal treatment for all customers of a financial institution and to avoid the financial institutions from being used for illegal purposes. In 1970, Congress passed the Bank Secrecy Act in an attempt to prevent people from using banks for money laundering. This act required banks to report any individual to the Internal Revenue Service for any money transaction over $10,000. Although the Bank Secrecy Act aided the monitoring of asset movement by an individual, it did very little to monitor the banks and other stakeholders of the financial industry. There was very little enforcement of laws that regulated the financial industry. Although the financial industry had some regulations that govern the industry, it did not do much to enforce the laws. The financial industry was pretty much left to regulate itself with very little checks and balances. The lack of checks and balances left top management of some financial institutions to engage in fraudulent activities which almost collapsed the American economy in the 21st century.

Perhaps the swiftest response to the financial crisis was the Sarbanes-Oxley Act of 2002 (SOX). Although SOX is arranged into eleven titles, the most important sections in regards to compliance are titles 302, 401, 404, 409, 802, and 906. Most of the compliance sections are divided into areas holding management, executives, and board members responsible for reporting and assuring the accuracy of organizations' financial reports. Section 302 of the act relates to corporate responsibility for financial reports. This section outlines the guidelines and the individuals required to sign the corporate financial report. The section also holds the signing officers responsible for any inaccurate information that may appear on the financial report. In addition, the section also requires the organization to assure the accuracy of the financial information on the report to reflect the health and condition of the organization. Further the section also explains that

no internal process of any organization can be used as a replacement function for this section. It forces organizations to use and follow this act strictly without any alternatives. While this may be a good way to assign responsibility and accountability to those involved in generating a corporate financial report, it does not take into consideration the cost on the organization and also the difficulties in assuring the accuracy of the data used for the report in a big corporation. Some corporations have a complex financial system involving different people at different levels and the input of wrong information may not easily be tracked to the source of the issue. Section 802 of the act imposes penalties including up to 20 years imprisonment for altering, destroying, mutilating, concealing, falsifying records, documents or tangible objects with intent to obstruct contaminate an investigation. Perhaps this proposed punishment will compel organizations to be truthful and accurate.

Although SOX implementation and execution may at first appear straight forward, it does not provide strict guidelines to achieve compliance. The law simply provides organizational requirements and penalties for noncompliance, but leaves the details to oversight bodies and the impacted organizations. SOX also ignores the global nature of financial operations and the possibility of having to comply with other nation's laws. Most regulatory laws govern only a country and are valid only within the country. With the massive data breach occurring and the lack of international laws across the globe, compliance requirements puts the burden on the financial institutes to comply with different regulations in different countries. This is very confusing and costly for most organizations that therefore turn to expert organizations whose expertise is in compliance. However organizations that turn to a vendor are still held responsible for any wrongdoing.

Regulations can have positive impacts when they compel organizations to comply with recognized security standards. However regulators must consider the impacts of broad legislation across the diverse organizations operating in the financial industry. Regulators must consider the cost organizations incur because companies often pass these costs on to consumers. Regulations often contain complicated language, requiring legal teams to sift through and interpret. However lawyers do not bear the responsibility for ensuring regulatory compliance. Regulations are not always convenient for organizations because they slow performance and add a hierarchy of processes into already-established organizational procedures. Achieving compliance often proves a difficult challenge because many organizations lack the resources to fully understand and therefore fully comply with complex regulatory frameworks.

CONCLUSION

The financial industry represents an enormous assortment of firms, agencies, and institutions with operations ranging from small, community banks to massive, international corporations. Managing the financial sector in the U.S. presents a herculean task to lawmakers and regulators charged with its oversight. Information technology, growing from a service enabler into a fundamental pillar of the financial industry, presents a new array of challenges as state and national level officials attempt to cope with cybersecurity risks, vulnerabilities, and cyber-crime threats. Their efforts have resulted in both carefully constructed and haphazardly fashioned legislation; they have manifested in landmark bills, including GLBA, SOX, and Dodd-Frank. Regulations can provide needed checks against careless behavior and necessary countermeasures

against fraudulent practices. Compliance adds value, highlighting areas for improvement throughout industry and aiding firms in securing their internal processes. However, regulations also carry the potential to burden the financial industry with duplication of effort and complex reporting schemes. Such measures prove counterproductive when only massive corporations with the resources to retain large legal and regulatory departments can survive in a tumultuous regulatory environment. Regulators must approach the financial industry with an even keel, leveraging strong Congressional oversight where necessary, while eliminating unnecessary burdens that stifle financial growth.

REFERENCES

Blauner, C. (2013). Developing a Framework to Improve Infrastructure Cybersecurity. Financial Services Sector Coordinating Council. Retrieved from http://www.fsscc.org/fsscc/news/2013/FSSCC-Response-NIST CybersecurityFramework.pdf

Davenport, T. (2004). Small banks say Sec. 404 forcing sale. American Banker, 169(227), 9-10.

Fitzgerald, J. (2012). Coping with the burdens of Dodd-Frank. Massachusetts Banker, 2012(4), 17-20.

Gingrich, N. & Kralik, D. W. (2008, November 5). Repeal Sarbanes-Oxley. The San Francisco Chronicle. Retrieved from http://www.sfgate.com/politics/article/ Repeal-Sarbanes-Oxley-3186747.php

Greenberg, P. (2012, August 20). Security Breach Notification Laws. National Conference of State Legislatures. Retrieved from http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

Harris, D. (2003). Privacy rule catches dealers off guard. Automotive News, 77(6039), 24

Klitch, S. (2012, September 17). Community banks and the JOBS Act. Idaho BusinessReview. Retrieved from http://idahobusinessreview.com/2012/09/17/community-banks-and-the-jobs-act/

Naber, J. D. (2008). Community bank audit's changing role. Connecticut Banking, 2008(1), 4-15

Rouse, M. (2013, May). Federal Information Security Management Act (FISMA).

TechTarget. Retrieved from http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act

Saucer, C. (2009, October, 23). Impact of Gramm-Leach-Bliley still debated 10 years later. Business Wire. Retrieved from http://www.reuters.com/article/2009/10 /23/idUS205297+23-Oct-2009+BW20091023

Scarborough, M. (2007). Casey-Landry testifies on Sarbanes-Oxley. Community Banker, 16(7), 18.

Snow, G. (2011). Statement before the House Financial Services CommitteeSubcommittee on Financial Institutions and Consumer Credit. Retrieved from http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector

Stevens, G. (2012). Data Security Breach Notification Laws. Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/misc/R42475.pdf

U.S. Federal Trade Commission. (2002). How to comply with the privacy of consumer financial information rule of the Gramm-Leach-Bliley Act. Retrieved from http://business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

U.S. Securities and Exchange Commission. (2011). CF Disclosure Guidance: Topic No. 2, Cybersecurity. Retrieved from http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

U.S. Department of Treasury. (2010). Banking and Finance Sector-Specific Plan: An Annex to the National Infrastructure. Retrieved from http://www.dhs.gov/sites/ default/files/publications/nipp-ssp-banking-and-finance-2010.pdf

Yu, A. (2012). Regulatory financial reform: Impact of Dodd-Frank Act on IT compliance. Rutgers Computer & Technology Law Journal, 38(2), 254-276