Bloomberg BNA

BNA's Banking Report™

DATA SECURITY

Risk Management

Data Security Considerations for FinTech Companies

By Ian C. Wildgoose Brown

I. Introduction; the General Rule

Businesses that straddle the worlds of finance and technology are subject to a regulatory patchwork that is only increasing in complexity as governments take a greater interest in privacy, data security and consumer protection.[1] As these two worlds converge, an increasing number of businesses will become subject to existing regulatory regimes as well as new initiatives from government agencies and industry players. Whether your business deals with individual or institutional customers, you are likely subject to a variety of legal and practical constraints in operating your business.

Data security and privacy standards for companies in the financial sector are generally well-settled, at least in theory. Companies generally must maintain reasonable procedures to protect sensitive information. However, this determination is highly context-specific: whether your security practices are reasonable depends on the nature and size of your business, the types of information you collect or have access to, the data security tools available to you based on your company's resources, and the particular security risks your business is likely to face.[2] In addition to this general rule, there are a number of statutes that impose specific obligations on certain types of businesses operating in this space.

II. Are You a "Financial Institution"?

The term ''financial institution'' is defined broadly under many of the laws that apply to the finance industry. In general, financial institutions include traditional commercial and investment banks as well as money services businesses such as money transmitters, cheque cashers, and sellers or issuers of stored value. However, companies like Facebook, which operate in apparently unrelated spaces, are warning in their disclosure documents that they could be subject to these laws.[3] Whether your business is subject to these laws depends on the substance of your company's activities.

[1] *Privacy, Technology and the Law*, United States Senate Committee on the Judiciary, http://www.judiciary.senate.gov/about/subcommittees/privacytechnology.cfm. Sen. Patrick Leahy, Chairman of the Senate Judiciary Committee, has set up a new Subcommittee on Privacy, Technology and the Law.

Ian C. Wildgoose Brown is an associate in the Transactional Department (Corporate) at WilmerHale. He is also a member of the firm's FinTech Group. Mr. Wildgoose Brown has a general corporate practice with an emphasis on mergers and acquisitions and capital markets transactions for companies at all stages of growth.

[2] Burke Kappler, *Protecting Personal Information – Know Why*, Bureau of Consumer Protection – FTC (October 2007), http://business.ftc.gov/documents/art08-protecting-personal-information-know-why.

[3] Facebook, Inc., Amendment no. 8 to Registration Statement on Form S-1, file no. 333-179287, as filed with the Securities and Exchange Commission on May 16, 2012, *available at* http://www.sec.gov/Archives/edgar/data/1326801/000119312512235588/d287954ds1a.htm.

 ISSN 0891-0634

For example, the Gramm-Leach-Bliley Act (which cross-references to the Bank Holding Company Act of 1956) imposes its data security and data-sharing standards on businesses that engage in general categories of ''financial'' activities. These activities include safeguarding or transacting in money or securities, lending, insuring, or providing financial, investment, or economic advice.[4] A patchwork of state ''money transmitter'' laws in states such as New York, New Jersey, Connecticut, Massachusetts and California supplement applicable federal laws. These state laws typically apply to non-bank companies engaging in activities within the state that facilitate consumer payments via funds that are kept, retrieved and transferred electronically—such as selling, issuing or exchanging ''payment instruments'' (substitutes for cash or value-holders), receiving money for transmission or transmitting money, and handling information connected with transactions in money or payment instruments. (Companies such as Facebook, Amazon, Google and PayPal are licensed money transmitters in California[5] and other states.) These laws typically require companies to obtain a license to operate and impose audit and corresponding data retention and records requirements.

Further, liberal interpretation of the definition of ''financial institution'' by regulating agencies under a variety of laws could capture not only banks and traditional financial institutions but also the service providers they contract with. And whether or not you are directly regulated, if you provide services to financial institutions then you are contracting with counterparties who are—and who are thinking of their own privacy and data security obligations as they negotiate their contracts with you. Their duty to safeguard information extends to situations where an institution makes the information available to third-party service providers. This legal backdrop will influence your negotiations and will affect how potential institutional customers view your business and practices.

III. Potential Implications of Being a Financial Institution

Data security breaches can result in direct liability to your company. For example, regulations under the Gramm-Leach-Bliley Act (discussed above) place responsibility for data security directly with the board of directors. And the Sarbanes-Oxley Act (applicable to public companies) makes the CEO and CFO responsible.[6] Industry organizations such as the PCI Security Standards Council[7] may also supply practices that can be used to inform your standard of care as a service provider.

Recent enforcement activity by regulators has targeted compliance and other issues involving companies that work with financial institutions. The Consumer Financial Protection Bureau's activities are of particular note for FinTech companies. The CFPB's mandate is to focus on consumer protection in markets for consumer financial products and services. This mandate extends beyond banks and financial institutions alone[8]: the CFPB's early enforcement actions have encompassed practices of service providers.

Breaches can also involve the allocation of financial losses among separate commercial entities. Personal information stolen from you, as a service provider who holds confidential information on behalf of a financial institution you provide services to, may injure that financial institution. It may need to take costly action to protect its customers and prevent losses on fraudulent transactions as a result of the breach—and may experience reputational damages as well. Provisions in your contract may allocate responsibility for such costs, which can be significant in relation to the size of your business, since guidance issued by federal banking regulators requires financial institutions to consider what protective measures are needed to safeguard personal information they permit third-party service providers to use.[9] Case law also address such disputes.[10] Cases deal with such issues as allocation of losses arising from cardholder data stolen from a merchant who failed to comply with Visa's security procedures requiring merchants to delete information captured from the magnetic strip on Visa payment cards after processing the transactions. This potential liability raises the stakes in your negotiations with financial institutions, even if your business is not itself a ''financial institution''.

At the least your contract will include terms providing for some degree of ongoing oversight of your activities. The CFPB has announced its ''expectation'' that financial institutions oversee their service providers in a manner that ensures compliance with federal consumer financial protection law.[11] Similarly, in recently updated policy statements in its IT Examination Handbook,[12] the Federal Financial Institutions Examination Council reaffirmed that a financial institution's board of directors and management has a duty to ensure that activities by third-party service providers, including FinTech companies, are conducted in a safe and sound manner and in compliance with applicable laws and

[4] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801, et seq., available at http://www.ftc.gov/privacy/glbact/glboutline.htm; cf. Bank Holding Company Act of 1956, 12 U.S.C. § 1843(k) (''Engaging in Activities that are Financial in Nature''), available at http://www.fdic.gov/regulations/laws/rules/6000-500.html.

[5] Owen Thomas, *This Innovation-Killing California Law Could Get A Host Of Startups In Money Trouble*, Business Insider (July 11, 2012), http://www.businessinsider.com/california-money-transmitter-act-startups-2012-7.

[6] Sarbanes-Oxley Act of 2002, 15 U.S.C. §§ 1350, 7241.

[7] PCI Security Standards Council, https://www.pcisecuritystandards.org.

[8] Bill Hardekopf, *CFPB Announces Signiificant Enforcement Action Against Capital One*, Forbes.com (July 18, 2012), http://www.forbes.com/sites/moneybuilder/2012/07/18/cfpb-announces-significant-enforcement-action-against-capital-one/.

[9] See Rebecca S. Eisner, *Securing Private Information in Service Provider Arrangements: New Developments Shape Emerging U.S. Privacy Standards*, Practising Law Institute (2007).

[10] http://www.bloomberglaw.com/public/document/Sovereign_Bank_v_BJ_Wholesale_Club_et_al_Docket_No_0603392_3d_Cir

[11] Consumer Financial Protection Bureau, *Consumer Financial Protection Bureau to hold financial institutions and their service providers accountable* (April 13, 2012), http://www.consumerfinance.gov/pressreleases/consumer-financial-protection-bureau-to-hold-financial-institutions-and-their-service-providers-accountable/.

[12] Federal Financial Institutions Examination Council, *Supervision of Technology Service Providers: IT Examination Handbook* (October 2012), available at http://op.bna.com/bar.nsf/r?Open=jtin-96tn77.

  BBR ISSN 0891-0634

regulations. To this end the FFIEC recently published a revised version of its Supervision of Technology of Service Providers guidelines.[13] The FFIEC's focus in examining financial institutions is to ensure that weaknesses are addressed and risks are properly managed. Its examiners evaluate a financial institution's – or a technology service provider's – overall risk exposure and risk management performance. They apply a risk-based examination system based primarily on the following factors to determine overall levels of risk that technology service providers present to their client financial institutions:

- *Board oversight*. Level of involvement of the company's board.
- *Technical and managerial expertise*. Competence and proactive approach by management.
- *Policies and procedures*. Quality, adequacy, and operation of policies and procedures relating to technology risks and data security.
- *Audit and internal controls*. Quality, adequacy, and operation of audit and internal controls, including levels of complaints and incidents or ''red flags''.

These frameworks and priorities influence the way financial institutions should think about their relationships with technology service providers. Your data security processes and procedures can be a valuable marketing tool. But knowing the obligations and the standards of care that you or your counterparty are subject to should also inform your contract negotiations and can help you understand what you can or should agree to.

IV. Overview of Legal Requirements

There is no single comprehensive body of law on liability for data security breaches. Instead there is a patchwork of federal, state, and regulatory laws whose effects vary depending on context. But the following are certain key requirements imposed by various laws that you should be aware of as a player in the finance sector. In general, applicable law requires a process-based approach to the development and maintenance of a comprehensive security program. This means that the steps you take as a business to preempt privacy and data security breaches (as well as thoroughly documenting those steps) are of paramount importance in establishing your legal compliance.

Data access

Your company must have reasonable written policies and procedures to ensure the security and confidentiality of customer information and to protect against unauthorized access to or use of that information, both by third parties and your own employees.[14] Multiple federal agencies enforce these requirements, and have published interagency guidelines establishing standards in this area.[15] If your business falls within the definition of a ''financial institution'' but you are not regulated by a specific banking agency, you may nevertheless fall within the ambit of the FTC's Safeguards Rule,[16] which the FTC enforces based on similar principles.[17] However, your business will also be subject to common law requirements similarly flexible in scope. Class actions such as those brought against ChoicePoint in the early days of data security litigation are good examples. Those cases involved allegations both of failure to implement adequate security measures and of commensurate failure to timely and fully disclose the breaches once they occurred.[18] Unfortunately there are no hard-and-fast rules, and the determination is context-specific. For instance, one court[19] has decided that encryption of sensitive personal data is not a mandatory requirement in all circumstances, but another[20] imposed liability where no steps were taken to protect similar data from foreseeable risk of a security breach. And certain FTC settlements have resulted in express commitments from businesses to store data in a format that cannot be meaningfully interpreted if opened as a flat plain-text file, or in a location that is physically inaccessible to unauthorized persons or that is protected by a firewall.[21]

---

[13] The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Federal Regulatory Agencies' Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers* (October 2012), available at http://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf.

[14] Kappler, supra note 2; 15 U.S.C. 6805(b).

[15] The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness*, 66 Fed. Reg. 8616 (2001) (see also, e.g., 12 C.F.R. pt. 30 (2001)), available at http://www.fdic.gov/regulations/information/ebanking/66FR8615.pdf; Federal Trade Commission, *Standards for Safeguarding Customer Information*, 16 C.F.R. pt. 314 (2002), available at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[16] 16 C.F.R. pt. 314 (2002).

[17] Kappler, supra note 2.

[18] Goldberg v. ChoicePoint, Inc. No. BC329115, (Los Angeles Superior Ct., filed Feb. 18, 2005); Perry v. ChoicePoint, Inc. No. CV-05-1644 (C.D. Cal., filed March 4, 2005).

[19] http://www.bloomberglaw.com/public/document/Guin_v_Brazos_Higher_Education_Service_Corporation_Inc_et_al_Dock; see also Identity Theft, *Judge: Not Encrypting Private Data Not Negligent*, Cybercrime Law (February 16, 2006), http://www.cybercrimelaw.org/2006/02/16/.

[20] http://www.bloomberglaw.com/public/document/Bell_v_Michigan_Council_25_of_American_Federation_of_State_Employ; see also Philip L. Gordon and Jeffrey F. Davis, *Michigan Becomes the First State in the Nation to Open the Door to Potential Employer Liability for Workplace Identity Theft*, FindLaw.com (March 26, 2008), http://corporate.findlaw.com/litigation-disputes/michigan-becomes-the-first-state-in-the-nation-to-open-the-door.html.

[21] Development and Implementation of Customer Information Security Program, 12 C.F.R. pt. 30, Appendix B, Part III (2002), available at http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=669186773b886ffec3bbe2b0139b8b60&rgn=div9&view=text&node=12:1.0.1.1.28.0.9.7.15&idno=12; In the Matter of Ziff Davis Media Inc., Assurance of Discontinuance, para. 25 (eff. August 28, 2002), available at http://www.ag.ny.gov/sites/default/files/press-releases/archived/aug28a_02_attach.pdf; HIPAA Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Subpart C (§ 164.302 et seq.) (2003), available at http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-part164-subpartC.pdf.

Data retention

Government agencies do not only assess whether companies have established and are complying with appropriate policies, procedures, and processes that allow identification and reporting of suspicious activity. They also require assurance that companies can provide sufficient detail in reports to law enforcement agencies so that those reports are useful in investigating any suspicious transactions that are reported.[22] Data retention is a common area of regulation with this end in mind. For instance, public companies (some of which you might work with or provide services to) are subject to Sarbanes-Oxley, which imposes its own data retention standards.[23] And, as a private company, you should be ready for audits by federal or state regulatory agencies probing for weaknesses that they think may threaten consumers—audits that will center on an examination of your records and that will require you to explain any gaps.

Data disposal

The flip-side of effective data retention is appropriate data disposal. Keeping information you do not reasonably need to retain increases the likelihood of incurring liability in the event of a data security breach. Further, certain types of business are specifically targeted by legislators and regulators. For example, if your business involves collecting credit or consumer reports, then you are subject to the obligation to take various measures to prevent identity theft. Key among these requirements is having and complying with appropriate procedures relating to data disposal.[24]

Treatment consistent with promises

The Federal Trade Commission enforces rules requiring businesses to handle consumer information in a way that is consistent with their promises to their customers (for example, in an online privacy policy), in addition to its rules discouraging data security practices that create an unreasonable risk of harm to consumer data.[25] The FTC has used this law to charge firms with unfair or deceptive practices in the ways they manage the security of customer information they possess,[26] including FinTech companies such as ValueClick (which operated an e-commerce site).[27]

Disclosure of breaches

You have a general duty to disclose security breaches to those who may be adversely affected by any such breach. This duty is based primarily on state law,[28] but also on certain key cases[29] and federal agency guidelines.[30] The kind of event that triggers a disclosure obligation therefore varies depending on the rules specifically applicable to your business. This uncertainty reinforces the importance of having robust processes for detecting breaches that could obligate you to inform or warn your customers, the government, or others. And of course the existence of the laws themselves underscore the importance of taking steps to reduce risk of having to make a disclosure in the first place, thereby avoiding the reputational damage that could result.

The objective of these standards is generally to shield your company's systems and information against unauthorized access, use, disclosure, or transfer, but also against modification or alteration, processing, or accidental loss or destruction. In designing safeguards, you should remember that the source of threats to your data security can be internal as well as external to your organization.

There are further legal requirements that apply if your business touches the EU. EU law specifically creates an individual right of access to any controller of personal data, broadly and with regard to any data processing function.[31] Under a proposed new law, U.S. companies would have to ensure that use and storage of EU citizens' personal data affords the same level of protection that such citizens are afforded within the EU.[32]

---

[22] Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2010), available at http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf.

[23] David Bowser, *How to Learn to Love Sarbanes-Oxley*, CSO Online (December 1, 2005), http://www.csoonline.com/article/220717/how-to-learn-to-love-sarbanes-oxley

[24] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (2007), available at http://op.bna.com/bar.nsf/r?Open=jtin-96su8c, as amended; see also, e.g., FTC Identity Theft Rules, 16 C.F.R. pt. 681 (2007, as amended), available at http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=82715d598ccbc1fce543fea55ae47bc8&r=PART&n=16y1.0.1.6.79; FTC Disposal of Consumer Report Information and Records Rule, 16 C.F.R. pt. 682 (2004, as amended), available at http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=4d02857f8b718afe33ef45deabfa22f7&rgn=div5&view=text&node=16:1.0.1.6.80&idno=16.

[25] Federal Trade Commission Act, 15 U.S.C. 45(a)(1).

[26] Federal Trade Commission, *Gateway Learning Settles FTC Privacy Charges* (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm.

[27] Federal Trade Commission, *ValueClick to Pay $2.9 Million to Settle FTC Privacy Charges* (March 17, 2008), http://www.ftc.gov/opa/2008/03/vc.shtm; United States v. ValueClick Inc., No. CV-08-01711 (C.D. Cal., March 13, 2008) (FTC complaint), available at http://www.ftc.gov/os/caselist/0723111/080317complaint.pdf

[28] National Conference of State Legislatures, *State Security Breach Notification Laws* (last updated: August 20, 2012), http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx ("Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.").

[29] Goldberg v. ChoicePoint, Inc., No. BC329115 (L.A. Sup. Ct., filed February 18, 2005); Perry v. ChoicePoint, Inc., No. CV-05-1644 (C.D. Cal., filed March 4, 2005).

[30] Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 12 CFR pt. 30 (2005), available at http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20050323/attachment.pdf.

[31] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[32] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (January 25, 2012); see, e.g., id., Art. 2 ("Scope"), § 1 ("processing of personal data in

  BBR ISSN 0891-0634

V. Best Practices and Guidelines

It is important for your business to establish clear processes that effectively address data security issues. The cost of implementing security measures – particularly relative to the size of your business – is a factor in determining the reasonableness of your precautions.[33] However, no FinTech business is exempt from the standard and any breach will be evaluated in hindsight. Your focus should be on risk assessment, and on adopting security controls that are responsive to the particular threats your company faces.

Your board of directors should provide strategic oversight regarding information security policy and practices.[34] You should ensure that the board understands how critical information and information security is to your organization, and you should endorse the development and implementation of a comprehensive information security program. You should advocate your company's investment in information security and clearly document those investments as they occur. As a management team, a key procedural step is regularly reporting to the board on the adequacy and effectiveness of your company's program.

The obligations that apply to financial institutions in particular are supplemented by a set of practices, many of which are recommended by government or industry bodies, that can create ''good facts'' for your business as you try to establish that your data security practices are reasonable. The following is a general overview of some of these best practices.

Have an executive officer with dedicated data security responsibility. Some experts point to major companies' failure to place people in charge of data security in positions high-ranking enough in the corporate hierarchy.[35] Creating a flatter organizational structure presents FinTech companies with an opportunity to differentiate themselves from larger competitors by having a data security officer with direct access to his or her fellow management team and to the board. The EU is moving in this direction: one proposed directive would require all private sector companies with more than 250 employees, all private sector companies whose core activities involve regular monitoring of individuals, and all public authorities to formally appoint a data protection officer.[36]

Implement preconceived processes and procedures. Reduce in-the-moment thinking, increase automation and response.[37] Setting up internal data security controls improves your company's regulatory compliance[38] and allows financial institutions you work with to assure themselves that they are satisfying their own regulatory compliance obligations. The process[39] involves the following steps:

- *Asset assessment*. Identify those systems and information that need to be protected.
- *Risk assessment*. Regularly evaluate the particular threats to data security that you face (internal and external), the likelihood that those threats will come to pass, and the potential costs associated with those threats.
- *Development*. Develop and implement security measures designed to manage and control the specific risks you've identified in your risk assessment.
- *Education*. Educate your employees and contractors on an ongoing basis.
- *Monitoring and testing*. Ensure that your program is properly implemented and effective.
- *Review and adjustment*. Revise your program in light of your changing security needs.

Implement—and use—network security protections. Some companies that have access to sensitive information maintain strict policies on handling and transmitting data by employees, particularly through third-party servers.[40] Allowing confidential data to be stored outside your firewall creates opportunities for targeted eavesdropping (use of programs to analyze the way multiple programs running simultaneously on the same operating system share memory space)[41] or relay or man-in-the-middle attacks (real-time insertion between the reader/recipient of a message and the victim

---

the context of the activities of an establishment of a controller [of data] or a processor in the Union'').

[33] See, e.g., HIPAA Security Standards: General Rules, 45 C.F.R. 164.306(b)(2); GLB Security Regulations, 12 C.F.R. Pt. 30, App. B, §§ II.A, III.C; 44 U.S.C. §§ 3544(a)(2), (b)(2)(B); In the Matter of Microsoft Corporation, File No. 012 3240, Agreement Containing Consent Order, Section II (August 7, 2002), available at http://cobrands.docs.findlaw.com/hdocs/docs/ftc/ftcms080802stlmt.pdf; In the Matter of Ziff Davis Media Inc., Assurance of Discontinuance, para. 25 (eff. August 28, 2002), available at http://www.ag.ny.gov/sites/default/files/press-releases/archived/aug28a_02_attach.pdf.

[34] 12 C.F.R. pt. 30 Appendix B, Part III, supra note 21; see also F. William Conner and Arthur W. Coviello et al., *Information Security Governance: A Call to Action*, National Cyber Security Summit Task Force (April 2004), pp. 12–13, available at http://www.cyberpartnership.org/InfoSecGov4_04.pdf.

[35] Brian Krebs, *Making the Case for Security*, MIT Technology Review (June 2, 2011), available at http://www.technologyreview.com/news/424174/making-the-case-for-security/ (interview with Eugene Spafford).

[36] Thor Olavsrud, *Data Protection Officer Role Will Be Key If You Operate in the EU*, PCWorld (June 1, 2012), http://www.pcworld.com/businesscenter/article/256668/data_protection_officer_role_will_be_key_if_you_operate_in_the_eu.html

[37] Scott Berinato, *Safe Document Transfer: How to Secure the Paper Chain*, CSO Online (February 27, 2008), http://www.csoonline.com/article/221323/safe-document-transfer-how-to-secure-the-paper-chain.

[38] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (November 2011), available at http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; Federal Trade Commission, *Financial Institution and Customer Information: Complying with the Safeguards Rule* (April 2006), available at http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

[39] See, e.g., 12 C.F.R. pt. 30, App. B.

[40] Brian Bergstein, *IBM Faces the Perils of ''Bring Your Own Device''*, MIT Technology Review (May 21, 2012), http://www.technologyreview.com/news/427790/ibm-faces-the-perils-of-bring-your-own-device/.

[41] David Talbot, *Security in the Ether*, MIT Technology Review (December 21, 2009), http://www.technologyreview.com/featured-story/416804/security-in-the-ether/.

of the attack).[42] Imaginative, proactive strategies for incentivizing employees to follow seemingly-burdensome data security procedures can help address such potential risks.[43] Industry standards such as the Payment Card Industry Data Security Standard, summarized below,[44] provide useful guidelines for specific steps you can take.

- Build and maintain a secure network. Install and maintain a firewall configuration to protect sensitive data. Do not use vendor-supplied defaults for system passwords and other security parameters. Encrypt transmission of sensitive data across open, public networks. Use and regularly update anti-virus software.

- Implement strong access control measures. Restrict access to sensitive data by business need-to-know. Assign a unique ID to each person with computer access. Restrict physical access to sensitive data.

- Regularly monitor and test networks. Track and monitor all access to network resources and sensitive data. Regularly test security systems and processes. Monitor developments in security and processing software to avoid falling behind.[45]

Be cautious about the cloud. The financial sector has been seen as ripe for use of cloud computing, but such developments raise data security issues.[46] Public cloud services are becoming a favorite target of data thieves.[47] And such third-party servers may be compelled to give up data in response to a subpoena—potentially circumventing privacy laws[48] and thereby undermining customer confidence in your FinTech company in a way that is unrelated to your business and out of your control.

Monitor developments and learn from past events.[49] A legal standard based on reasonableness is a moving target. As data security practices change, and as technology and security threats evolve in tandem, the measures you will have to take will likewise evolve. Avoid succumbing to a false sense of security[50] by conducting periodic internal reviews and monitoring external developments and current events. Then take easily-documented and established steps in response to these reviews. For example, increasing numbers of online repositories of personal data are switching to HTTPS for their online presence/interface. This step is not yet broadly mandated, but settlements with certain key industry players, such as Google[51] and Twitter[52], have set the tone. The FTC has continued to provide updated guidance[53] on its priorities in the realm of privacy and data security. And as discussed above, new rules and standards from the CFPB and FFIEC affect, both directly and indirectly, the FinTech sector. As a FinTech company, you should monitor such practices and guidance, and implement those elements that are reasonably applicable to your business and reasonable in cost.

The consequences to your company's finances and reputation can be significant where any kind of personal data is compromised.[54] In short, data security is a process not a product.

VI. Conclusion

The financial sector's context-specific regulatory approach is likely to be put to the test as the balance of market power shifts between established financial institutions on the one hand and startups and nontraditional industry players on the other. Traditional financial institutions may now have the advantage in emerging markets such as mobile payments because they have proven security measures and solid reputations, but that could change quickly as new entrants challenge established players with new innovative offerings from equally powerful companies[55] and nimble software-as-a-service businesses[56] alike. But these newer or smaller players may not have the same experience dealing with and protecting sensitive information as they enter the finance industry. The problem is amplified with the increasing focus on mobile devices and the intersection of

---

[42] Keatron Evans, *Man In The Middle – Demystified*, InfoSec Institute (April 30, 2011), http://resources.infosecinstitute.com/man-in-the-middle-demystified/.

[43] L. Jean Camp, *Data Security Is a Risk-Management Problem*, MIT Technology Review (June 14, 2011), http://www.technologyreview.com/news/424291/data-security-is-a-risk-management-problem/.

[44] PCI Security Standards Council, *PCI Data Security Standards* (October 2010), available at https://www.pcisecuritystandards.org/security_standards/documents.php.

[45] Matt Hines, *Payment systems culprit in TJX heist*, InfoWorld (March 29, 2007), http://www.infoworld.com/d/security-central/payment-systems-culprit-in-tjx-heist-283.

[46] Talbot, supra note 41.

[47] Lucas Mearian, *Mobile Devices Bring Cloud Storage – and Security Risks – to Work*, PCWorld (June 10, 2012), http://www.pcworld.com/businesscenter/article/257276/mobile_devices_bring_cloud_storage_and_security_risks_to_work.html.

[48] Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 et seq. (mandating certain notice and justification requirements relating to government requests for financial information).

[49] Bill Brenner, *Slideshow: 15 words data breaches*, CSO Online (February 15, 2012), http://www.csoonline.com/slideshow/detail/31963/Slideshow—15-worst-data-breaches?source=csointcpt_15worst_ss#slide1.

[50] InfoSecurity, *Executive optimism misplaced as security standards slip* (September 21, 2012), http://www.infosecurity-magazine.com/view/28388/executive-optimism-misplaced-as-security-standards-slip-/.

[51] Sam Schillace, *Default https access for Gmail*, Official Gmail Blog (January 13, 2010), http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html#!/2010/01/default-https-access-for-gmail.html.

[52] RachaelRad (Twitter Comms), *We suggest using HTTPS for improved security. We're starting to turn this on by default for some users. More here: support.twitter.com/articles/48195. . .*, Twitter (August 23, 2011); based on a settlement with the FTC, Federal Trade Commission, *FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information* (March 11, 2011), http://www.ftc.gov/opa/2011/03/twitter.shtm.

[53] Federal Trade Commission, *FTC Issues Final Commission Report on Protecting Consumer Privacy* (March 26, 2012), http://ftc.gov/opa/2012/03/privacyframework.shtm.

[54] U.S. Department of Health and Human Services, *HHS settles HIPAA case with BCBST for $1.5 million* (March 13, 2012), http://www.hhs.gov/news/press/2012pres/03/20120313a.html.

[55] Cameron Scott, *Mobile Wallet Systems Could Hurt Brick-and-mortar Banks, Survey Suggests*, PCWorld (June 5, 2012), http://www.pcworld.com/businesscenter/article/256928/mobile_wallet_systems_could_hurt_brickandmortar_banks_survey_suggests.html

[56] Krebs, supra note 35.

  BBR ISSN 0891-0634

finance and tech in mobile payments: ''In addition to financial information, mobile devices store tremendous amounts of personal and commercial data that may attract both targeted and mass-scale attacks.''[57]

Responding to these constraints and adhering to best practices can have their own benefits in addition to reducing legal risks. The increasing prevalence of software-as-a-service businesses used by financial institutions and by other types of companies outsourcing their financial-related processes means that a single data security breach is amplified and raises the stakes for both you and your competitors.[58] A strong data security record is a valuable asset in an increasingly crowded marketplace.

[57] LOOKOUT MOBILE SECURITY, *State of Mobile Security 2012*, http://op.bna.com/bar.nsf/r?Open=jtin-96suth; LOOKOUT MOBILE SECURITY, *2011 Mobile Threat Report*.

[58] Krebs, supra note 35.