‘Reasonable security’: A moving target

Received (in revised form): 21st December, 2017

Elizabeth E. McGinn

Partner at Buckley Sandler LLP, assists financial institutions and corporations in identifying, evaluating, and managing the risks associated with cyber security, internal privacy, and information security practices, as well as those of third-party vendors. She advises clients on the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the General Data Protection Regulation (GDPR), the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule (TSR), the Health Insurance Portability and Accountability Act (HIPAA), security breach notification laws and other US state and federal privacy requirements. She has assisted clients in addressing data security incidents as well as developing policies and procedures, records retention schedules, and training materials. Elizabeth has been listed in *Legal 500* in 2013–18.

Partner, Buckley Sandler LLP, 1250 24th Street NW, Suite 700, Washington, DC 20037, USA
Tel: +1 202 349 7968; E-mail: emcginn@buckleysandler.com

James Shreve

is a partner and chair of Thompson Coburn’s Cybersecurity group serving as a trusted advisor to clients facing complex cybersecurity and privacy issues — particularly those in the country’s most highly regulated industries. A recognized thought leader in the fields of cybersecurity and privacy, he was recognized as a Next Generation Lawyer in Cyber Law (Data Protection and Privacy) in 2017 and 2018 by Legal 500 and was named ‘Associate to Watch’ in Chambers USA in 2015 and Chambers Global in 2016. Applying the law to rapidly changing technology and software capabilities, he provides clients with a profile of their potential risk, then works closely with executive leadership, legal, IT, and compliance information security teams to develop a comprehensive and practical plan for risk avoidance and responding to cyber and data-related issues.

Partner, Thompson Coburn LLP, 55 East Monroe Street, 37th Floor, Chicago, IL 60603, USA
Tel: +1 312 580 5087; E-mail: jshreve@thompsoncoburn.com

Margo H. K. Tank

is a Partner of DLA Piper, and focuses her practice on advising financial services companies, commercial enterprises and technology companies on the full spectrum of regulatory compliance matters related to the use of electronic signatures and records to enable digital transactions offered online and via mobile devices. Margo began her legal career as counsel to the US House of Representatives, Committee on Banking and Financial Services. She is currently counsel to the Electronic Signatures and Records Association, where she works to further electronic financial services policy before Congress and federal regulators. She has been recognized by *Legal 500* (2014–2017) in the area of Media, Technology and Telecoms — Technology: Cyber Law (Data Protection and Privacy).

DLA Piper LLP (US), 500 Eighth Street, NW, Washington, DC 20004, USA
Tel: +1 202 799 4170; E-mail: margo.tank@dlapiper.com

Abstract ‘Reasonable security’ for companies charged with protecting customer and employee data has evolved over the last 20 years. Previously, financial institutions had broader latitude on how to safeguard and adequately protect personally identifiable information (PII) under federal and state data protection laws. Today, legal and regulatory requirements and expectations regarding information data security controls are not only more prescriptive but continue to evolve as technology and those who seek to gain unauthorised access to personal information become more sophisticated. The

number of governmental entities involved in information security is also increasing in the US. No longer the exclusive domain of federal regulatory agencies, state legislatures and regulators and attorneys general are issuing requirements, providing guidance and enforcing state laws to ensure that companies employ 'reasonable security' when collecting, handling, storing, transferring and disposing PII.

KEYWORDS: reasonable security, GLBA, FTC, safeguards, personally identifiable information, PII, specificity, cyber security, data security, information security

THE GENESIS OF THE 'REASONABLE SECURITY' CONCEPT

The concept of 'reasonable security' for personal information maintained by financial institutions began with the Gramm-Leach-Bliley Act (GLBA). On 12th November, 1999, Congress enacted GLBA, a landmark privacy and data security law which required the federal financial regulatory agencies[1] to 'establish appropriate standards for the financial institutions subject to their jurisdiction relating to 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.'[2]

Under this authority, the federal financial regulatory agencies adopted the Safeguards Rule,[3] which introduced the concept of 'reasonableness' to information security requirements.[4] The Safeguards Rule requires that a financial institution 'develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [a financial institution's] size and complexity, the nature and scope of [a financial institution's] activities, and the sensitivity of any customer information at issue'.[5]

While Section 4 of the Safeguards Rule mandates certain elements for an information security programme, most of these elements are general in nature. One specific required element of the Safeguards Rule is a risk assessment. The financial institution must '[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks'.[6] Information security controls are to be based on the risks identified in the risk assessment and the financial institution must test or otherwise monitor the effectiveness of the controls. Financial institutions have operated under this risk-based approach for over 15 years.

FTC ACTIONS IN THE EARLY 2000S UNDER GLBA AND SECTION 5 OF THE FTC ACT TO CREATE REASONABLE SECURITY REQUIREMENTS

In 2004, the Federal Trade Commission (FTC) began to file complaints for alleged violations of the Safeguards Rule and, in doing so, clarified to some extent what was required for reasonable information security. Most early FTC enforcement actions under the Safeguards Rule asserted in the

complaint that the financial institution had made claims about information security practices that were not accurate. In later FTC actions, the complaints alleged that the financial institutions failed to implement reasonable policies and procedures to secure nonpublic personal information and that the failure constituted an unfair or deceptive act or practice.[7] The complaints described the general nature of the financial institution's alleged shortcomings, but did not include facts regarding what particular company practices violated the Safeguards Rule.

Nearly all information security actions by the FTC resulted in consent orders, in which the financial institution did not admit to any violations of law. While the consent orders did not provide specific facts regarding the alleged conduct *or* why the conduct did not rise to the level of 'reasonable security',[8] the FTC consent orders alleged the companies': 1) failure to oversee third parties; 2) lack of appropriate employee training; and 3) inadequate incorporation of security into the design process for products and services. As a result, the consent orders required the financial institutions to implement: 1) continuous systems monitoring (including user monitoring); 2) segmentation of the financial institution's network; 3) controls for remote access to the financial institution's system; and 4) controls for third party access to systems and nonpublic personal information. These requirements illustrated components of what the FTC considered to be 'reasonable security'.[9]

The FTC also has applied the concept of 'reasonable security' outside the scope of GLBA under the agency's general authority in Section 5 of the FTC Act. In *FTC v. Wyndham*, the FTC sued a global hotel company for allegedly failing to adequately safeguard its computer network, allowing hackers to access customer information. Among Wyndham's arguments, the company challenged the FTC's authority to enforce information security requirements through unfairness actions, arguing that FTC complaints and guidance do not provide adequate notice of what security practices are considered 'reasonable'. The Third Circuit rejected this type of argument in a 2015 holding that the FTC's issuances as a whole provided notice on the agency's views on requisite components of reasonable security. The importance of this case is twofold. First, the Third Circuit decision affirmed the FTC's use of Section 5 to challenge unreasonable data security practices. Second, this case and the FTC's numerous other data security settlements offer guidance to companies as to what the FTC considers 'reasonable security'.

CONTRASTING THE DIFFERENT APPROACH OF THE FFIEC

The reasonableness approach of the FTC stands in contrast with that of the Federal Financial Institutions Examination Council (FFIEC), a formal interagency body set up to prescribe uniform principles, standards and report forms for the federal examination of financial institutions.[10] The FFIEC's mission is to promote safety and soundness in areas rather than consumer protection or compliance with legal requirements such as GLBA. To further the FFIEC's mission, the interagency body in 2003 began to issue a series of handbooks (IT Examination Handbooks) for use by the FFIEC member agencies in conducting examinations of the information technology systems of regulated financial institutions.

The IT Examination Handbooks include a booklet on Information Security that provides 'guidance to examiners and addresses factors necessary to assess the level of security risks to a financial institution's information systems' and helps 'examiners evaluate the adequacy of the information security program's integration into overall risk management'.[11] The Information Security booklet, first issued in 2006, took a significantly different approach from the FTC Safeguards Rule by covering a broad

range of specific information security controls and including significant technical details regarding the controls. The original version of the Information Security booklet contained 136 pages and covered several specific security topics.[12] This compares to the FTC Safeguards Rule, which is less than three pages and includes only four, more general topics. Although the Safeguards Rule itself is considerably shorter and less detailed than the FFIEC Information Security booklet, through the FTC's line of enforcement actions and more recent guidance discussed below, the Safeguards Rule is becoming similar to the FFIEC approach to information security.

STATE INVOLVEMENT COMMENCES WITH THE ENACTMENT OF BREACH NOTICE LAWS

As the FTC commenced enforcement actions under the Safeguards Rule, states wanted to do their part and began to focus on information security and started to enact data security breach notice laws. California passed the first such law in 2003.[13] After two high-profile security incidents in early 2005, other states began enacting similar security breach notice laws, all based in varying degrees on the California model.[14]

To date, 15 states have enacted some form of information security provisions as part of the state breach notice statute. Several states also require entities to have a reasonable process for the destruction of materials containing personal information relating to state residents.[15] While some of these laws mandated entities to employ reasonable measures to protect personal information,[16] with the exception of Massachusetts and Nevada discussed in more detail below, they did not specify what constitutes 'reasonable security' steps.

In February 2009, Massachusetts enacted the *Standards for the Protection of Personal Information of Residents of the Commonwealth*.[17] The Massachusetts regulation marked a significant change in the approach to data security regulation. Entities would be expected to include as part of their mandated 'comprehensive information security program' certain specific controls. This regulation, enacted under the state's breach notice law, contained several requirements beyond those expressly required under the federal Safeguards Rule. For example, the Massachusetts mandated controls include:

1. User authentication protocols;
2. Data access controls;
3. Encryption of personal information stored on portable devices or sent across public networks;
4. Software patching;
5. Systems monitoring;
6. Firewall protection;
7. Virus protections;
8. Employee training.

The Massachusetts regulation also applied beyond the financial services sector by covering *any* entity that possessed personal information relating to a state resident.

Following Massachusetts, in the same year, Nevada enacted a requirement for *any* entity (not just financial institutions) that 'handles, collects, disseminates or otherwise deals with nonpublic personal information', to encrypt personal information transferred beyond the entity's secure system.[18] The Nevada requirement went beyond the Massachusetts regulation's encryption requirement by specifically defining the term 'encryption'.[19]

REASONABLE SECURITY REQUIREMENTS CONTINUE TO DEVELOP OUTSIDE THE RULE-MAKING PROCESS

The specificity as to what is considered 'reasonable security' has continued to accelerate at both federal and state level. While the FTC has continued to pursue data security enforcement actions, the agency increasingly also uses reports and guidance

to communicate expectations about data security.

For example, in November 2013, the FTC held a public workshop called *Internet of Things: Privacy & Security in a Connected World*. This workshop examined privacy and security issues posed by new internet-connected devices. In January 2015, the FTC released the *Internet of Things – Privacy & Security in a Connected World* report ('IoT Report'), in which the agency provided several information security recommendations for mobile and other connected devices. The report recommended that a reasonable information security programme would include at least six elements:

1. Implement 'security by design' to incorporate security into devices from the outset;
2. Address security at the appropriate level in the organisation and through employee training;
3. Retain service providers capable of maintaining reasonable security and oversight of those service providers;
4. Employ defence-in-depth for systems with significant risk;
5. Utilise reasonable access control measures to prevent unauthorised access to a consumer's device, data or network; and
6. Monitor security issues through the lifecycle of a product and as feasible patch known vulnerabilities.[20]

The public workshop and IoT Report are noteworthy because both delve deep into recent technology developments and include significant input from technologists, academics, industry representatives and consumer advocates.

In June 2015, the FTC expanded its efforts to help businesses protect consumers' information through a new initiative providing them with more information on data security. This initiative, called *Start with Security,* included new guidance for businesses from lessons learned in the more than 50 data security cases brought by the agency. The guidance document issued, *Start with Security: A Guide for Business,* listed ten key security steps to effective information security drawn from the alleged facts in the FTC's information security cases.[21] The document provided a way for companies to understand the lessons learned from previous cases. It included references to past enforcement actions and a plain-language explanation of the security principles at issue.

In October 2016, the FTC issued further security guidance for businesses with a document entitled *Protecting Personal Information: A Guide for Business*. The guide articulated that a sound information security plan is based on five key principles. These five principles restated points made in the FTC's *Start with Security* guidance but included additional concrete guidance on particular topics.[22]

More recently, starting on 21st July, 2017, the FTC followed up the *Start with Security* series with a similarly titled series of business blog posts, *Stick with Security*. In this new series, the FTC issued posts for several weeks, each focusing on a security topic. The ten topics followed the *Start with Security* series, but provided more descriptions and examples.

The FTC guidance of the last few years clarifies and ties together the 15 years of enforcement actions regarding what constitutes 'reasonable security'. Given the cumulative nature of this body of law, the concept of 'reasonable security' will continue to become more specific through additional enforcement actions.

THE CONSUMER FINANCIAL PROTECTION BUREAU'S WARNING SHOT

Finally, in March 2016, the Consumer Financial Protection Bureau (CFPB) stepped into the cyber security enforcement area by announcing its first enforcement action related to the adequacy of a company's

data security practice, citing its authority under the Dodd-Frank Act to protect consumers against deceptive practices and false representations. The CFPB took action against online payment platform Dwolla for allegedly deceiving consumers about its data security practices and the safety of its online payment system. Specifically, the CFPB asserted that Dwolla misrepresented its data security practices by: 1) falsely claiming its data security practices 'exceed' or 'surpass' industry standards; and 2) falsely claiming its 'information is securely encrypted and stored'. The CFPB ordered Dwolla to pay a $100,000 penalty and fix its security practices. Notably — and unlike FTC consent orders — the Dwolla consent order listed the information security areas where the CFPB asserted the company failed to implement 'reasonable and appropriate' practices, including risk assessments, employee training and testing software.[23] Although the consent order does not cite failures by the entity's board of directors, the required remedial steps include specific duties for the board. The CFPB required that the board: 1) review all materials to be submitted by the company to the CFPB; 2) have ultimate responsibility for compliance with all consumer financial laws and the consent order; 3) authorise all actions required for compliance with the consent order; 4) require timely reporting by company management on the status of compliance obligations; and 5) require appropriate corrective actions for any material noncompliance with board directives.

The consent order highlights regulators' focus on risk assessments, written security plans, employee training, software testing and representations about security standards.

CALIFORNIA AND NEW YORK NOW REQUIRE SPECIFIED SECURITY CONTROLS

In the last few years, California and New York have issued regulations and guidance that include more specific information security requirements. In February 2016, the California Attorney General's Office issued the *California Data Breach Report* (Breach Report), a report on security breach notifications the office received and the nature of the incidents. The Breach Report indicated that the Attorney General's Office expected at a minimum that a 'reasonable security' programme would include all 20 security controls contained in the Center for Internet Security's (CIS) Critical Security Controls, a well-known voluntary industry best practices standard.[24] The Attorney General's Report stated that '[t]he failure to implement all the [CIS] Controls that apply to an organization's environment constitutes a lack of "reasonable security"'. Similar to the FTC actions, the Breach Report was issued by an enforcement agency and was not a rule making subject to public comment.

In March 2017, the New York Department of Financial Services (NYDFS) finalised a groundbreaking cyber security regulation ('Cybersecurity Requirements for Financial Services Companies') applicable to all financial institutions subject to the regulatory authority of NYDFS.[25] The NYDFS regulation covers many of the same topics as the Massachusetts regulation as well as the recent FTC issuances. However, compared to the Massachusetts regulation, the requirements of the NYDFS regulation are more specific and cover a broader range of security topics, such as the retention of a Chief Information Security Officer and encryption for nonpublic information (not just nonpublic personal information), both in transit and at rest.

Notably, NYDFS has touted the regulation as a model for legislation and regulations for other states. Already in November 2017, the National Association of Insurance Commissioners (NAIC) used many provisions from the NYDFS regulation to draft its own model cyber security law.[26]

The involvement of more states could lead to a nationwide collection of laws

and regulations where the requirements are different or possibly inconsistent. The adoption process by states of the NAIC model cyber security law could be indicative of how states will move forward. If states adopt the model largely unchanged, the result would be a generally uniform, but more specific standard than under the Safeguard Rule. If states adopt the model law with certain variations, the resulting patchwork of specific and different information security standards would greatly increase the compliance burden.

SUGGESTED COMPLIANCE STEPS FOR COMPANIES

In light of the trend toward more stringent and specific information security controls, the following are some suggested compliance steps:

1. Perform a risk assessment to determine what information security controls may need to be implemented. While some specific controls are being mandated or expected by regulators, many legal and regulatory requirements around information security remain risk-based. A risk assessment helps in determining the nature and scope of a company's risks to information and the controls that are appropriate to address those risks.
2. Consider using established security standards as a tool to develop information security policies and procedures. Using well-known standards such as ISO 27001, the FFIEC Cybersecurity Assessment Tool or the NIST Cybersecurity Framework can provide a measure for an information security programme. Use of such standards allows companies to demonstrate specific safeguards and controls that are in place to secure information and networks.
3. Think about which controls work and which may not. If a particular mandated or regulator-expected control is not effective or feasible for a company, consider documenting why and think about alternative controls that may be better suited for use in the company's information security programme.
4. Consider using outside resources to provide insight and perspective. Consultants and outside counsel often advise a range of clients about compliance and frequently interact with regulators regarding information security compliance. These interactions with clients and regulators allow the consultants and counsel to give perspective on trends in approaches to risks and controls, allowing useful insight for clients.

Notes and References

1. The Dodd-Frank Act changed the allocation of regulatory authority for portions of GLBA. Prior to the Dodd-Frank Act, both the privacy and information security provisions of GLBA were addressed by the financial regulators for all financial institutions under their jurisdiction. The Dodd-Frank generally gave authority over GLBA privacy requirements, with certain exceptions, to the Consumer Financial Protection Bureau (CFPB). Regulatory and enforcement authority for information security requirements in GLBA was left with the FTC and the bank regulatory agencies and not given to the CFPB.
2. 15 U.S.C. § 6801(b).
3. The federal bank regulatory agencies jointly issued a version of the Safeguards Rule for financial institutions subject to their authority and the FTC issued a version of the Safeguards Rule covering financial institutions not subject to the authority of the other agencies. The versions of the rule are substantially similar. This article references the FTC version of the Safeguards Rule.
4. See, eg, 16 C.F.R. § 314. The Safeguards Rule uses the term 'reasonable' or 'reasonably' four times in the less than 800-word rule.
5. 16 C.F.R. § 314.4(b).
6. *Ibid.*, note 5.
7. See, eg, Sunbelt Lending Services, Inc., Docket No. C-4129 (Jan. 3, 2005); Nationwide Mortgage Group, Inc. Docket No. 9319 (Nov. 9, 2004).
8. See, eg, Premier Capital Lending, Inc. Docket No. C-4241 (Dec. 10, 2008).
9. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); see also, Binkley, J. William, Fair Notice or Unfair Practices: Due Process in FTC Data Security Enforcement after Wyndham, 31 Berkeley Tech. L.J. 1079, 1091 (2016).

10. The current FFIEC member agencies are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau.
11. FFIEC (July 2006), 'Information Technology Examination Handbook, Information Security', available at https://ithandbook.ffiec.gov/media/222209/ffiec_itbooklet_informationsecurity-2006.pdf (accessed 5th February, 2018).
12. The Information Security booklet included sections on access controls, physical and environmental protection, encryption, malicious code prevention, systems development, acquisition and maintenance, personnel security, data security, service provider oversight, business continuity considerations, and insurance. The current version of the Information Security booklet, issued in September 2016, has been shortened to 96 pages, but covers additional topics.
13. Cal. Civil Code § 1798.82 *et seq*.
14. The proliferation has continued such that only two states, Alabama and South Dakota, do not have breach notification laws.
15. See Ark. Code Ann. § 4-110-104; N.J. Stat. Ann. § 56.8-162.
16. See Or. Rev. Stat. Ann. § 646A.622; Tex. Bus. & Com. Code § 521.052.
17. 201 C.M.R. § 17.01 *et seq*.
18. Nev. Rev. Stat. § 603A.215.
19. The Nevada statute defines encryption as 'the protection of data in electronic or optical form, in storage or in transit, using:
    1. An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data;
    2. Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology; and
    3. Any other technology or method identified by the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration in regulations adopted pursuant to NRS 603A.217'. Nev. Rev. Stat. § 603A.215(4)(b).
20. FTC (January 2015), 'Internet of Things: Privacy & Security in a Connected World', available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (accessed 5th February, 2018).
21. The ten listed principles were:
    1. Start with security.
    2. Control access to data sensibly.
    3. Require secure passwords and authentication.
    4. Store sensitive personal information securely and protect it during transmission.
    5. Segment your network and monitor who's trying to get in and out.
    6. Secure remote access to your network.
    7. Apply sound security practices when developing new products.
    8. Make sure your service providers implement reasonable security measures.
    9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
    10. Secure paper, physical media, and devices.

    The 'Start with Security' guidance is available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (accessed 5th February, 2018).
22. FTC (October 2016), 'Protecting Personal Information: A Guide for Business' available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (accessed 5th February, 2018).
23. In re Dwolla, Inc., File No. 2016-CFPB-0007 (Feb. 27, 2016).
24. The California statutes contain a requirement that those possessing nonpublic personal information relating to a state resident must employ reasonable security to safeguard the information. Cal. Civ. Code § 1798.81.5.
25. Notably, even companies that are not subject to the NYDFS cyber security regulation may benefit from reviewing its requirements because other states and regulators in other subject areas may look to the regulation in promulgating their own cyber security requirements.
26. See Statement by DFS Superintendent Maria T. Vullo Regarding the NAIC Adoption of the Insurance Data Security Model Law (24th October, 2017), available at http://www.dfs.ny.gov/about/statements/st1710241.htm (accessed 5th February, 2018).