Bloomberg BNA

Privacy and Security Law Report®

FTC Enforcement

In the absence of legislation, companies must continue to look to FTC cases such as Wyndham, enforcement actions and guidance, such as ''Start with Security: A Guide for Business,'' as well as the Gramm-Leach-Bliley Act and the NIST cybersecurity framework for insights on what amounts to reasonable data security, the author writes.

An Overview of FTC Hot Buttons in Cybersecurity Programs for 2016

By Richard A. Blunk

Introduction

A recent U.S. Court of Appeals for the Third Circuit ruling has validated the Federal Trade Commission's (FTC) approach of noting what deficiencies in cybersecurity program render such a program to be ''unreasonable'' and, hence, legally insufficient. [1]Although this approach does not present a safe harbor to achieve the goal of satisfying the requirement that all such cybersecurity programs be reasonable and should be read in conjunction with other industry cybersecurity standards and practices, practitioners in this area are advised to structure, implement, maintain and update their programs in light of the general principals stressed by the FTC in these enforcement actions as well as the specific noted deficiencies.

Reasonable Data Security?

In 2012, FTC sued Wyndham Worldwide Corp., a global hospitality company, and three of its subsidiaries alleging that those parties had failed to maintain reasonable and appropriate data security practices for sensitive customer data.[2] These overall failures led to three data breaches at Wyndham hotels in less than two years, resulting in millions of dollars of fraudulent charges on consumers' credit and debit cards—and the transfer of hundreds of thousands of consumers' account information to a website registered in Russia.

The FTC challenged Wyndham's failure to comply with its own privacy policy as an impermissible ''deceptive'' act. More interestingly for present purposes, however, the FTC also claimed that that fundamental inadequacy of Wyndham's cybersecurity program—its failure to provide ''reasonable'' protection—also constituted a similarly prohibited ''unfair'' business practice. This was a predictable position for the FTC to take since Wyndham did not include several rudimentary components typically found in acceptable cybersecurity programs. These deficiencies, the FTC claimed, ''unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.'' Highlighted deficiencies included failing to use readily available security measures, such as firewalls; storing credit card information in clear text; failing to implement rea-

[1] *FTC v. Wyndham Worldwide Corp.*, 2015 BL 271793, 799 F.3d 236 (3d Cir. 2015) (14 PVLR 1592, 9/7/15)

Richard A. Blunk is the Managing Director and General Counsel, Thermopylae Ventures, LLC

[2] *FTC v. Wyndham Worldwide Corp.*, 2014 BL 94785, 10 F. Supp. 3d 602 (D.N.J. 2014) (11 PVLR 1069, 7/2/12)

 ISSN 1538-3423

sonable information security procedures prior to connecting local computer networks to corporate-level networks; failing to address known security vulnerabilities on servers; using default user names and passwords for access to servers; failing to require employees to use complex user IDs and passwords to access company servers; failing to inventory computers to appropriately manage the network; failing to maintain reasonable security measures to monitor unauthorized computer access; failing to conduct security investigations; and failing to reasonably limit third-party access to company networks and computers.

The FTC contended that the failure to maintain such reasonable and appropriate data security practices for sensitive customer data—such as their as credit and debit card numbers in the *Wyndham* case, and to comply with its privacy policy are deceptive and unfair acts prohibited by the FTC Act since they ''cause [] or [are] likely to cause substantial injury to consumers which [are] reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'' In essence, then the U.S. Court of Appeals for the Third Circuit held that the FTC has the authority to regulate data security standards for participants in commercial transactions involving such sensitive personal information even in the absence of detailed regulations that set out all of the FTC's requirements for such programs. The court reached this second holding after noting that practitioners in this areas could have taken guidance from holdings in approximately 50 cybersecurity enforcement actions taken by the FTC since initiating this campaign in 2002.

Predictably, this decision has been derided by business interests since they note—correctly so—that *Wyndham* does not require the FTC's adoption of a useful safe harbor to ensure compliance. Experts differ, these parties claim, in identifying which cybersecurity practices should be broadly accepted as being ''reasonable'' and hence widely implemented in order to secure compliance. Differences also exist between differing types of companies and technologies, which is particularly troubling since the stakes for non-compliance seem to increase with each successive breach. The FTC, these critics claim, is either moving the goal post or at least not telling the players where the current goal post is.

Consumer privacy advocates hailed the *Wyndham* decision by noting that the FTC is particularly well equipped to serve as privacy regulator in commercial situations involving sensitive consumer data.

Consumer privacy advocates, such as the Electronic Privacy Information Center, on the other hand, hailed the *Wyndham* decision by noting that the FTC is particularly well equipped to serve as privacy regulator in commercial situations involving sensitive consumer data. According to this independent non-profit privacy research center, the FTC should continue to aggressively enforce its consent decrees in order to ensure the protection of consumer privacy rights, especially in light of the increasing sophistication, frequency and impact of recent cyberattacks.

Siding with these consumer privacy advocates, the FTC has recently published an overview of the key points—or ''lessons learned''—noted in its recent enforcement actions, the absences of which led the FTC to determine such cybersecurity programs to be ''unreasonable'' and hence legally flawed.[3] Understanding these principals, while briefly reviewing the precise deficiencies noted in these enforcement actions[4], should be a primary resource for all practitioners whose clients are involved in financial transactions subject to the Gramm-Leach-Bliley Act (GLBA). Many of those requirements—as set out below—should be self-evident and others will provide helpful technological advice which, if heeded, should help companies from committing what the FTC characterizes as ''basic, fundamental security missteps.''

Always be mindful of the FTC's guiding principles. Reasonable data security is based on broad principles beginning with a thoughtful analysis of the following key issues: understanding what consumer information the company has and what employees or third parties have access to it; being guided by the legitimate business needs, limiting the information the company collects and retains from consumers; protecting the information the entity maintains by assessing risks and implementing protections in certain key areas such as physical security, electronic security, employee training, and oversight of service providers; properly disposing of information that they no longer need; and having a continuously improving plan to respond to security incidents, should they occur.

Control general access to data. Once a company has concluded that it does have a legitimate business need for specific consumer information, it must take reasonable steps to keep that sensitive data secure by restricting access, and limiting administrative access, to that information. In this regard, the FTC has advised that a company should segment its servers so that unauthorized access to one areas on the network does not automatically compromise the security of all areas; apply readily available security measures—such as firewalls or isolated payment card systems—to control and monitor access to the network from wireless access points, between computers on the company network and the Internet; limit employee access to, and copying of, personal information based on such employee's role; restrict third party access to personal information based on business need, for example, by restricting access based on IP address, granting temporary access privileges, or similar procedures; establish an employee login page that is unknown to consumers and separate from the customer/end user login page; and restrict the

[3] Federal Trade Commission, ''Start with Security: A Guide for Business'' (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. (14 PVLR 1236, 7/6/15)

[4] *See, e.g.*, P. Bailin, ''Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices'' (Sept. 19, 2014), *available at* https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf *and* ''Federal Trade Commission 2014 Privacy and Data Security Update,'' *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

  PVLR ISSN 1538-3423

number of files on which data can be stored in order to simplify compliance with data use limitations and deletion procedures.

Require secure passwords and authentication for individual access. This step should be self-evident and should include requiring the use of complex or unique passwords, storing passwords securely—not on a Post-It-Note on the chief information officer's workstation. FTC enforcement actions have shown their strong preference for using strong, hard-to-guess user IDs and passwords; prohibiting the use of common dictionary words; forbidding the use of the same word or a close variant of the word for both the password and the ID, and denying a user the ability to create credentials that he or she already employs elsewhere on the network; requiring periodic changes of user credentials for customers and employees with access to sensitive personal information; suspending user credentials and/or disabling administrative passwords after a reasonable number of unsuccessful login attempts; prohibiting the use of default passwords or the sharing of user credential; prohibiting the storage of administrative passwords in plain text on computers, in cookies, or in personal e-mail accounts; and, implementing procedures to authenticate the identity of users who wish to create new credentials to access additional systems or programs that contain personal information.

Store sensitive personal information securely and protect it during transmission. Maintaining security for this sensitive information throughout the entire life cycle of such data is imperative. For example, all storage should include retaining information in areas within a segmented network that provide optimal security. Of special note is the emphasis the FTC has placed on the use of acceptable encryption in the majority of these enforcement actions. The goal should be to render personal information to be unusable, unreadable or indecipherable by transmitting sensitive and personal information, including user credentials and financial account and credit card information, securely in either encrypted format or through cryptographic protocols such as Transparent Layer Security or Secure Sockets Layer. In two recent enforcement actions, the FTC found that mobile apps failed to properly authenticate and secure the transmission of customer data from the mobile apps.

Secure remote access to your network. Companies should analyze this step in light of the old adage that a chain is only as strong as its weakest link. It does little good to provide excellent security for activities done at the office without also providing endpoint security for remote access. A guiding principal for both remote and in-office use, the access afforded to users across the network should be driven by the information they need to access in order to perform their duties, while noting that very few personnel need to have access to, and/or administrative control over, the entire network. Two recent FTC enforcement actions have been especially critical of inadequate authentication and security measures used in data transmissions from corporate mobile apps.

Monitor who's trying to get in, across and out of the network. All cybersecurity experts understand the absolute necessity of being able to properly monitor all such activity by ensuring endpoint security, putting sensible access limits in place as well as through the use of intrusion detection systems and other methods to monitor logins for suspicious activity. Since technology advances so rapidly in this space, companies are reminded of the general advice of the FTC to use ''readily available'' technology and practices in this, and all other, key aspects of a reasonable data security program.

Review and ensure compliance by software and other products used by the company. All of these programs and products should comply with corporate data security procedures. Such a well-structured program would require the implementation of appropriate checks and controls on the review and testing of software and products intended for internal use; adherence to well-known, commonly-accepted secure programming practices, including those described in the product's operating system technical guides, and performing perform security reviews and testing of software and products at key points throughout the development cycle.

Apply sound security practices when developing new products. Given the potential value that new products may have to the companies that develop them, caution must be exercised in order to prevent data breaches during the development process. Suggestions include training the company's engineers in secure coding, following platform guidelines for security, verifying that extant privacy and security features function properly and testing for commonly known and reasonably foreseeable vulnerabilities.

Contractually obligate third party service providers to implement reasonable security measures. Given the continuing outsourcing of various corporate functions, companies should candidly discuss their security expectations with potential vendors, take reasonable steps to select providers that are able and willing to implement appropriate security measures in order to satisfy those expectations and verify their compliance with those goals. FTC enforcement cases suggest that the outsourcing contract should expressly require such service providers to implement and maintain appropriate safeguards for consumers' personal information; provide for reasonable oversight of the service providers' security practices and their employees' handling of personal information; adequately verify, through monitoring and assessments, that these service providers actually implement reasonable and appropriate security measures to protect personal information; and request and review relevant information—such as the results of audits and other security assessments—concerning the efficiency of the ongoing operation of a service provider's security practices and whether they satisfy both an-

nounced corporate expectations but contractual obligations as well.

Unless and until a safe harbor is set out either by the courts and/or by the FTC, the development, implementation and continuous improvements required to have a "reasonable" cybersecurity system must understand, and adopt the guidance provided by cases, such as *Wyndham*.

Secure paper, physical media and other devices that may contain sensitive information. Of course, the storage, use and transmission of sensitive information on the network must be supported by similar efforts in connection with all other media, such as paperwork, hard drives, laptops, flash drives and disks, on which such sensitive information may be stored. Companies would be well advised to adequately encrypt all sensitive and personal information retained on in-store networks, back-up tapes, or other portable media devices.

Dispose of sensitive data securely. Companies should also have policies in place to determine how long the company has a legitimate need to retain and use such data and destroy it after those legitimate needs have been satisfied. Here companies should also assess their retention obligations under regulatory and contractual obligations in order to properly render such information unreadable or otherwise secure in the course of disposal after compliance with all of those requirements have been satisfied.

Put procedures in place to keep the system current while also addressing significant vulnerabilities that may arise. Given the increasing sophistication and frequency of cyberattacks, companies must make a concerted effort to not only address new threats as they arise but to proactively plan for reasonably foreseeable future attacks. Key precautions noted by the FTC include updating and patching third-party software, heeding credible security warnings and quickly fixing them and developing a corporate culture that recognizes the importance of maintaining the appropriate level of vigilance and response on an ongoing basis. Practioneers should always remember that what's reasonable today may not be reasonable tomorrow.

While helpful, it is important to note that neither the ''lessons learned'' from these recent enforcement actions, the requirements of the GLBA or case law such as *Wyndham* are not meant to, and do not provide an exhaustive list of all of the necessary cybersecurity precautions that must be included in order for a cybersecurity program to be ''reasonable.'' These FTC enforcement actions note what deficiencies rendered a particular program to be ''unreasonable'' but even when viewed in their entirety, they do not provide, as critics repeatedly and correctly point out, the precise requirements for an acceptable safe harbor.

As a result, practitioners are well advised to continue to monitor the rapidly evolving case law in this area as well as industry guidelines, such as the GLBA Safeguards Rule with a special emphasis on its requirements for employee training and management such as obtaining references for prospective new hires, referring all request for customer information to a specified person, implementing appropriate disciplinary measures for violations of corporate cybersecurity policies and immediately the steps necessary to prevent recently terminated employees to obtain any access to the network. In addition, practitioners should apply several of the major obligations included in the Cybersecurity Framework adopted by the National Institute of Science and Technology (NIST) such as those requiring the determination of the company's risk tolerance, the adoption of corporate governance mechanisms that buttress compliance with current cybersecurity protections and much more details guidance on intrusion acknowledgment and assessment that are not set out in either the FTC policy pronouncements or highlighted in the FTC enforcement actions.

The recent resolution of the *Wyndham* case shows some movement towards a safe harbor but that a substantial amount of subjectivity remains. In mid-December 2015, Wyndham agreed to implement and maintain for 20 years an enterprise wide ''comprehensive information security program that is *reasonably designed* (emphasis added) to protect the security, confidentiality and integrity'' of customer credit card and related data. Compliance is based, to a significant degree, upon satisfying the Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures. Aspects of the FTC's requirements under this standard were explicitly described in the order. For example, Wyndham is to identify an employee that will be accountable for this program. This person is to be involved in a risk assessment that must include (i) employee training and management; (ii) a review of network and software; and (iii) prevention, detection, and response to attacks, intrusions and other systems failures. However, a good bit of the current uncertainty remains in areas such as how to select and oversee third party data processing vendors. Compliance must be by both an independent, qualified expert in this field as well as by senior corporate officials, and additional recordkeeping requirements were imposed.

Lessons

Unless and until a safe harbor is set out either by the courts and/or by the FTC, the development, implementation and continuous improvements required to have a ''reasonable'' cybersecurity system must understand, and adopt the guidance provided by cases, such as *Wyndham*, recent FTC enforcement actions, the GLBA Rule and the NIST Framework. Given the increasing sophistication of cyberattacks, bank regulatory counsel must retain an active role in making sure that senior management and the Board remain apprise of the evolving nature of cybersecurity compliance.

  PVLR ISSN 1538-3423