THE FTC SAFEGUARDS RULE: INFORMATION SECURITY PROGRAM ELEMENTS

BY
MELISSA J. KRASNOW

Melissa Krasnow is a partner at VLP Law Group LLP, Minneapolis, and an International Association of Privacy Professionals Certified Information Privacy Professional/US (CIPP/US).

Visit www.competitionpolicyinternational.com for access to these articles and more!

THE FTC SAFEGUARDS RULE: INFORMATION SECURITY PROGRAM ELEMENTS

By Melissa J. Krasnow

This article describes the elements of an information security program under the Federal Trade Commission Final Rule regarding Standards for Safeguarding Customer Information (the "FTC Rule"). While the effective date of the FTC Rule was January 10, 2022, certain information security program elements become effective as of December 9, 2022. This article also highlights differences between the FTC Rule information security program elements with counterparts under the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies. Financial institutions to which the FTC Rule applies should assess the extent to which their information security programs satisfy the elements of an information security program under the FTC Rule, identify, and address any gaps and document the foregoing. Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs.

01
INTRODUCTION

The federal and state law requirements for information security programs continue to evolve. Examples include the Federal Trade Commission ("FTC") Final Rule regarding Standards for Safeguarding Customer Information (the "FTC Rule") and the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies (collectively, the "NY DFS Requirements").[2] This article describes the elements of an information security program under the FTC Rule and highlights differences between these elements with counterparts under the NY DFS Requirements. Financial institutions to which the FTC Rule applies should assess the extent to which their information security programs (for example, employee coordinators, risk assessments, safeguards, testing, service provider oversight and evaluation and adjustment, among other things), satisfy the elements of an information security program under the FTC Rule, identify, and address any gaps and document the foregoing. Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs.

02
APPLICATION

The FTC Rule applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction.[3] *Financial institution* means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k).[4] An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.[5] Financial institutions include, without limitation, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission and entities acting as finders.[6] *Customer information* means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.[7] *Nonpublic personal information* means personally identifiable financial information and any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.[8] *Personally identifiable financial information* means any information that a consumer provides to the financial institution to obtain a financial product or service therefrom, about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer or that the financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.[9] In addition to defining financial institution, customer information, nonpublic personal information, and personally identifiable financial information, the FTC Rule also defines authorized user, consumer, customer, encryption, financial product or service, financial service, information security program, information system, multifactor authentication, penetration testing, security event and service provider, among other things.[10]

The NY DFS Requirements apply to a covered entity, meaning any person operating under or required to operate under a license, registration, charter, certificate, per-

2 86 Fed. Reg. 70,272 et seq. (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314) and 23 NYCRR pt. 500.

3 16 CFR § 314.1(b).

4 16 CFR § 314.2(h)(1).

5 16 CFR § 314.2(h)(1).

6 16 CFR § 314.1(b).

7 16 CFR § 314.2(d).

8 16 CFR § 314.2(l)(1).

9 16 CFR § 314.2(n)(1).

10 16 CFR § 314.2.

mit, accreditation or similar authorization under the New York Banking Law, the New York Insurance Law or the New York Financial Services Law.[11] *Nonpublic information* under the NY DFS Requirements means all electronic information that is not publicly available information and is: (1) business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity, (2) any information concerning an individual which because of name, number, personal mark or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account or (v) biometric records, (3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual or (iii) payment for the provision of health care to any individual.[12] In addition to defining a covered entity and nonpublic information, NY DFS Requirements also define cybersecurity event, information system, multi-factor authentication, risk assessment, risk-based authentication and third party service provider(s), among other things.[13]

03
INFORMATION SECURITY PROGRAM ELEMENTS

FTC Rule information security program elements include a qualified individual, risk assessments, safeguards, testing, training and personnel, oversight of service providers, evaluation and adjustment, an incident response plan and board reporting.[14] Certain of these elements do not apply to financial institutions that maintain customer information concerning fewer than 5,000 consumers ("Excepted Financial Institutions") as described below.[15] The NY DFS Requirements contain a number of exemptions (i.e. 23 NYCRR § 500.19).[16] Although the FTC Rule became effective January 10, 2022, certain information security program elements become effective as of December 9, 2022 as described below.[17]

A. Qualified Individual

Under the FTC Rule, a qualified individual (not limited to the Chief Information Security Officer ("CISO"), as required by the NY DFS Requirements) that is responsible for overseeing, implementing, and enforcing the information security program ("Qualified Individual") must be designated.[18] The foregoing becomes effective as of December 9, 2022.[19]

B. Risk Assessments

The FTC Rule requires the information security program to be based on a written risk assessment that identifies 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 that assesses the sufficiency of any safeguards in place to control these risks and must include criteria and requirements as follows, except for Excepted Financial Institutions.[20] The criteria and requirements must include: criteria for the evaluation and categorization of identified security risks or threats that the financial institution faces, criteria for the assessment of the confidentiality, integrity and availability of the financial institution's information systems and customer information, including the adequacy of the existing controls in the context of the

11 23 NYCRR § 500.1(c).

12 23 NYCRR § 500.1(g).

13 23 NYCRR § 500.1.

14 16 CFR § 314.4.

15 16 CFR § 314.6.

16 23 NYCRR § 500.19.

17 86 Fed. Reg. 70,272 et seq. (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314).

18 16 CFR § 314.4(a) and 23 NYCRR § 500.4(a).

19 16 CFR § 314.5.

20 16 CFR § 314.4(b)(1) and 16 CFR § 314.6.

identified risks or threats the financial institution faces, and requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.[21] The foregoing becomes effective as of December 9, 2022.[22] Also, additional risk assessments must be performed periodically.[23]

> *The FTC Rule requires the information security program to be based on a written risk assessment that identifies reasonably foreseeable internal and external risks to the security*

The NY DFS Requirements require periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program, carried out in accordance with written policies and procedures, which must be documented and updated as reasonably necessary to address changes to such information systems, nonpublic information or business operations, allow for revision of controls to respond to technological developments and evolving threats and consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.[24]

C. Safeguards

The FTC Rule requires safeguards to control the risks identified through risk assessment to be designed and implemented, which become effective as of December 9, 2022, as follows.[25]

Access Controls. Under the FTC Rule, access controls must be implemented and periodically reviewed access controls, including technical and, as appropriate, physical controls to: authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information and limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information.[26] As part of a cybersecurity program under the NY DFS Requirements, based on the risk assessment, user access privileges to information systems that provide access to nonpublic information must be limited and periodically reviewed.[27]

Identification and Management of Data, Personnel, Devices, Systems, and Facilities. The FTC Rule requires the data, personnel, devices, systems, and facilities that enable achievement of business purposes in accordance with their relative importance to business objectives and risk strategy to be identified and managed.[28]

Encryption. Under the FTC Rule, all customer information held or transmitted both in transit over external networks and at rest must be protected by encryption or, to the extent that encryption is determined to be infeasible, be secured using effective alternative compensating controls reviewed and approved by the Qualified Individual.[29] The FTC Rule defines *encryption as* the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.[30] As part of a cybersecurity program under the NY DFS Requirements, based on the risk assessment, controls, including encryption, must be implemented to protect nonpublic information and, to the extent that encryption of nonpublic information is determined to be infeasible, such nonpublic information must be secured using alternative compensating controls, which must be reviewed and approved by the CISO.[31] To the extent utilized, the feasibility of encryption and effectiveness of the

21 16 CFR § 314.4(b)(1).

22 16 CFR § 314.5.

23 16 CFR § 314.4(b)(2).

24 23 NYCRR § 500.9(a)-(b).

25 16 CFR § 314.4(c) and 16 CFR § 314.5.

26 16 CFR § 314.4(c)(1).

27 23 NYCRR § 500.7.

28 16 CFR § 314.4(c)(2).

29 16 CFR § 314.4(c)(3).

30 16 CFR § 314.2(f).

31 23 NYCRR § 500.15(a).

compensating controls must be reviewed by the CISO at least annually.[32]

Application Security. The FTC Rule requires secure development practices for in-house developed applications utilized for transmitting, accessing or storing customer information and procedures for evaluating, assessing or testing the security of externally developed applications utilized to transmit, access or store customer information to be adopted.[33] The NY DFS Requirements require a cybersecurity program to include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized and procedures for evaluating, assessing or testing the security of externally developed applications utilized within the context of the covered entity's technology environment and all such procedures, guidelines and standards must be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee).[34]

Multi-Factor Authentication. The FTC Rule requires multi-factor authentication for any individual accessing any information system to be implemented, unless the Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls.[35] The FTC Rule defines *multi-factor authentication* as authentication through verification of at least two of the following types of authentication factors: knowledge factors (such as a password), possession factors (such as a token) or inherence factors (such as biometric characteristics).[36]

The NY DFS Requirements define *multi-factor authentication* slightly differently from the FTC Rule: authentication through verification of at least two of the following types of authentication factors: knowledge factors (such as a password), possession factors (such as a token or text message on a mobile phone) or inherence factors (such as a biometric characteristic).[37] Multi-factor authentication must be utilized for any individual accessing internal networks from an external network, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls and, based on the risk assessment, effective controls, which may include multi-factor authentication or risk-based authentication, must be used to protect against unauthorized access to nonpublic information or information systems.[38]

> *The FTC Rule requires multi-factor authentication for any individual accessing any information system to be implemented*

Data Disposal. Under the FTC Rule, procedures must be developed, implemented and maintained for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained and the financial institution's data retention policy must be periodically reviewed to minimize the unnecessary retention of data.[39] As part of a cybersecurity program under the NY DFS Requirements, there must be policies and procedures for the secure disposal on a periodic basis of nonpublic information under 23 NYCRR § 500.1(g)(2)-(3).[40]

Change Management. The FTC Rule requires adopting procedures for change management.[41]

Logging. Policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users must be implemented under the

32 23 NYCRR § 500.15(b).

33 16 CFR § 314.4(c)(4).

34 23 NYCRR § 500.8.

35 16 CFR § 314.4(c)(5).

36 16 CFR § 314.2(k).

37 23 NYCRR § 500.1(f).

38 23 NYCRR § 500.12.

39 16 CFR § 314.4(c)(6).

40 23 NYCRR § 500.13.

41 16 CFR § 314.4(c)(7).

FTC Rule.[42] The NY DFS Requirements require such policies, procedures, and controls to be risk-based.[43]

> *The FTC Rule requires adopting procedures for change management*

D. Testing

The FTC Rule requires regular testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems and, for information systems, monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments.[44] The FTC Rule defines p*enetration testing* as a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside the financial institution's information systems (the NY DFS Requirements use the same definition regarding a covered entity).[45]

Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the following must be conducted: annual penetration testing of the information systems determined each given year based on relevant identified risks in accordance with the risk assessment and vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in the information systems based on the risk assessment, at least every six months and whenever there are material changes to operations or business arrangements and whenever there are circumstances known or for which there is a reason to know may have a material impact on the information security program, except for Excepted Financial Institutions.[46] The foregoing becomes effective as of December 9, 2022.[47]

The NY DFS Requirements require the cybersecurity program for a covered entity to include monitoring and testing, developed in accordance with the risk assessment, designed to assess the effectiveness of the cybersecurity program, including continuous monitoring or periodic penetration testing and vulnerability assessments.[48] Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities, a covered entity must conduct annual penetration testing of the covered entity's information systems determined each given year based on relevant identified risks in accordance with the risk assessment and bi-annual vulnerability assessments, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the covered entity's information systems based on the risk assessment.[49]

E. Training and Personnel

The FTC Rule requires implementing policies and procedures to ensure that personnel are able to enact the information security program by: (1) providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment; (2) utilizing qualified information security personnel employed by the financial institution or an affiliate or service provider sufficient to manage information security risks and to perform or oversee the information security program; (3) providing information security personnel with security updates and training sufficient to address relevant security risks and (4) verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.[50] The foregoing becomes effective as of December 9, 2022.[51] The NY DFS Requirements are comparable to the foregoing.[52]

42 16 CFR § 314.4(c)(8).

43 23 NYCRR § 500.14(a).

44 16 CFR § 314.4(d)(1).

45 16 CFR § 314.2(m) and 23 NYCRR § 500.1(h).

46 16 CFR § 314.4(d)(2) and 16 CFR § 314.6.

47 16 CFR § 314.5.

48 23 NYCRR § 500.5.

49 23 NYCRR § 500.5.

50 16 CFR § 314.4(e).

51 16 CFR § 314.5.

52 23 NYCRR § 500.14 and § 500.10.

F. Oversight of Service Providers

The FTC Rule requires oversight of service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.[53] The FTC Rule defines *service provider* as any person or entity that receives, maintains, processes or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to 16 CFR Part 314.[54] The FTC Rule also requires overseeing service providers by periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.[55] The foregoing becomes effective as of December 9, 2022.[56]

The NY DFS Requirements define *third party service provider* as a person that is not an affiliate of the covered entity, provides services to the covered entity and maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity.[57]

Subject to a specified exception, the NY DFS Requirements require implementing written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers, which must be based on the risk assessment, and address to the extent applicable: (1) identification and risk assessment of third party service providers, (2) minimum cybersecurity practices required to be met by such third party service providers in order for them to do business with the covered entity, (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third party service providers and (4) periodic assessment of such third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.[58]

Such policies and procedures must include relevant guidelines for due diligence and/or contractual protections relating to third party service providers including to the extent applicable guidelines addressing: (1) the third party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by 23 NYCRR § 500.12, to limit access to relevant information systems and nonpublic information, (2) the third party service provider's policies and procedures for use of encryption as required by 23 NYCRR § 500.15 to protect nonpublic information in transit and at rest, (3) notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or nonpublic information being held by the third party service provider and (4) representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information.[59]

> ***The FTC Rule requires implementing policies and procedures to ensure that personnel are able to enact the information security program***

G. Evaluation and Adjustment

Under the FTC Rule, the information security program must be evaluated and adjusted in light of the results of the required testing and monitoring, any material changes to operations or business arrangements. the results of risk assessments or any other circumstances known or for which there is reason to know may have a material impact on the information security program.[60]

H. Incident Response Plan

The FTC Rule requires establishing a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity or availability of customer information in the financial institution's control and must address: (1) the

53 16 CFR § 314.4(f)(1)-(2).

54 16 CFR § 314.2(q).

55 16 CFR § 314.4(f)(3).

56 16 CFR § 314.5.

57 23 NYCRR § 500.1(n).

58 23 NYCRR § 500.11(a) and (c).

59 23 NYCRR § 500.11(b).

60 16 CFR § 314.4(g).

goals of the incident response plan, (2) the internal processes for responding to a security event, (3) the definition of clear roles, responsibilities and levels of decision-making authority, (4) external and internal communications and information sharing, (5) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls, (6) documentation and reporting regarding security events and related incident response activities and (7) the evaluation and revision as necessary of the incident response plan following a security event, except for Excepted Financial Institutions.[61] The foregoing becomes effective as of December 9, 2022.[62]

As part of a cybersecurity program under the NY DFS Requirements, a written incident response plan (containing content comparable to the foregoing under the FTC Rule) must be established, designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the information systems or the continuing functionality of any aspect of business or operations.[63]

> *The FTC Rule requires the Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body*

I. Board Reporting

The FTC Rule requires the Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body (if no such board or body exists, such report must be timely presented to a senior officer responsible for the information security program) and the report must include the following information: the overall status of the information security program and compliance with 16 CFR Part 314 and material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto and recommendations for changes in the information security program, except for Excepted Financial Institutions.[64]

The foregoing becomes effective as of December 9, 2022.[65] Under the NY DFS Requirements, the CISO must report in writing at least annually to the board of directors or equivalent governing body on the cybersecurity program and material cybersecurity risks (if no such board or body exists, such report must be timely presented to a senior officer responsible for the cybersecurity program).[66] The CISO must consider to the extent applicable: (1) the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems, (2) the covered entity's cybersecurity policies and procedures, (3) material cybersecurity risks to the covered entity, (4) overall effectiveness of the cybersecurity program and (5) material cybersecurity events involving the covered entity during the time period addressed by the report.[67]

04 CONCLUSION

Considering the January 10, 2022 effective date of the FTC Rule and certain information security program elements becoming effective as of December 9, 2022, financial institutions to which the FTC Rule applies should assess the extent to which their information security programs satisfy the elements of an information security program under the FTC Rule, identify, and address any gaps and document the foregoing. Others to which the FTC Rule does not apply also may choose to assess where their programs, policies, and practices, among other things, stand in light of evolving federal and state law requirements for information security programs.

61 16 CFR § 314.4(h) and 16 CFR § 314.6.

62 16 CFR § 314.5.

63 23 NYCRR § 500.16.

64 16 CFR § 314.4(i) and 16 CFR § 314.6.

65 16 CFR § 314.5.

66 23 NYCRR § 500.4(b).

67 23 NYCRR § 500.4(b).

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL