July 13, 2020 · Washington, DC

Information Security & Financial Institutions

An FTC Workshop on GLB Safeguards

Opening Remarks

David Lincicum
Federal Trade Commission
Division of Privacy & Identity Protection

Background

- GLB was enacted in 1999.
- The Safeguards Rule was enacted in 2002 and became effective on May 23, 2003.
- No changes have been made to the rule since then.
- After seeking comments, the Commission issued a Notice of Proposed Rulemaking on March 5, 2019.

Current Rule

- Applies to Customer Information held by Financial Institutions.
- Applies to all Customer Information either of Customers of the Financial Institution or Customers of other Financial Institutions that provided the information.
- Requires the Financial Institution to have a Comprehensive Information Security Plan.

Current Rule

- **Comprehensive Information Security Program**
  - Must be appropriate to:
    - FI's size and complexity
    - The nature and scope of activities.
    - Sensitivity of Customer Information at issue.
  - Must :
    - Designate an employee or employees to coordinate.
    - Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.
    - Assess the sufficiency of Safeguards in place to control risks.
    - Address employee training and management; information systems; and detecting, preventing and responding to attacks.

Current Rule

- Financial Institutions must:
  - Design safeguards to control risks and regularly test the effectiveness of those safeguards.
  - Oversee service providers by selecting ones that are capable of maintaining appropriate safeguards and requiring them by contract to maintain those safeguards.
  - Evaluate and adjust the Information Security Plan based on:
    - Results of testing.
    - Any material Changes to operations.
    - Any other circumstances that you have reason to know will materially impact your information security program.

Proposed Rule

- Seeks to maintain the flexibility of the current Rule, while providing more guidance about the contents of a Information Security Program.

- Would provide clear requirements for financial institutions while still allowing the financial institution to create a program that is adapted to its particular needs.

- Is based on New York's Cybersecurity Regulations, 23 NYCRR 500, which were implemented in early 2017.

Proposed Rule

- Still based on creation of a Comprehensive Information Security Program based on a risk assessment that is suited to the size and complexity of the financial institution and the sensitivity of the Customer Information involved.
- Includes more detailed requirements for the plan.
- Almost all of the requirements are process based and adaptable.
- Financial Institutions that maintain less customer information would be exempted from some requirements.

Proposed Rule

- Under the proposed rule, Financial Institutions must:
  - Designate one qualified individual to be responsible for overseeing the program.
    - Only changes are requiring one person to have responsibility and the addition of the word "qualified."
    - Uses term "CISO" but this is not intended to require a specific set of qualifications. "Qualified" will vary based on size and complexity of the network.
  - Base the program on a written risk assessment that must include certain criteria for determining risk and address how the program will address those risks.
  - Periodically perform additional risk assessments – it is not something that can be done once and forgotten.
  - Regularly test or otherwise monitor the effectiveness of the program. Either through continuous monitoring, or through:
    - Annual penetration testing and
    - Biannual vulnerability assessments.

Proposed Rule

Training

- Under the proposed rule, Financial Institutions must:
  - Provide security awareness training to personnel
  - Utilize qualified information security personnel, either employees or through a service provider.
  - Train those security personnel and verify that they take steps to maintain current knowledge.

Proposed Rule

- Under the proposed rule, Financial Institutions must
  - Oversee service providers as under the current rule and periodically assess those providers.
  - Evaluate and adjust your program as under the current rule.
  - Establish a written incident response plan.
  - Require person in charge of program to provide annual written report to board of directors (or equivalent governing body) regarding the status of the information security program.

Proposed Rule

- Under the proposed Rule, the Information Security Program would need to address certain elements:
  - Access Controls: Controls to limit access to information only to authorized individuals.
  - "Information Inventory": Must identify and manage the data, personnel, devices and systems and facilities and how they are connected to risk strategy.
  - Secure development practices: Applies to security of applications developed to handle Customer information, and must evaluate security of third-party applications.

Proposed Rule

- Audit Trails: Must include audit trails that will allow the detection of security events.
- Disposal: Must have procedures for secure disposal of information that is no longer necessary for legitimate business purposes.
- Change Management: Must have procedures for handling changes to the system, including connecting to other networks or databases, and changes to the structure of the network.
- Monitor activity of authorized users: Systems for making sure that authorized users are not misusing information.

Proposed Rule

- Two elements that would require more specific aspects of the program:
  - Encryption
  - Multifactor Authentication.
- Both allow alternate controls if approved by person in charge of program.
- Both allow flexibility in implementation.

Proposed Encryption Requirement

- Would require that all customer information held or transmitted be encrypted both in transit over external networks and at rest.

- Points to note:
  - Would apply only to customer information.
  - Would only apply to transmitted information when it is transmitted over external networks.
  - If financial institution determines that encryption is not feasible, they may use effective alternative compensating controls reviewed and approved by person in charge of program.

Proposed MFA Requirement

- Would require multifactor authentication for any individual accessing customer information.

- Must include at least two of three factors:
  - Knowledge Factor (“Things you know”) – Passwords, biographical information.
  - Possession Factor (“Things you have”) – Tokens, possession of devices.
  - Inherence Factor (“Things you are”) – biometric characteristics such as fingerprints or voice.

- Reasonable equivalent or more secure access controls may be used if person in charge of program approves in writing.

Proposed Exception

- Financial institutions that maintain information about fewer than 5,000 consumers would be exempted from most of the written requirements.

Workshop

- We are speaking to people with direct experience providing information security to organizations and other experts in the field.
- Looking to gather concrete information on the costs and benefits of practices set forth in the proposed rule.
- We are particularly interested in the costs and scalability to smaller businesses.

Schedule

9:30–10:30 - The Costs and Benefits of Information Security Programs

10:45-11:45 - Information Security Programs and Smaller Businesses

1:00-2:00 - Continuous Monitoring, Penetration, and Vulnerability Testing

2:15–3:15 - Accountability, Risk Management, and Governance of Information Security Programs

3:30-4:30 - Encryption and Multifactor Authentication

Questions and Comments

- Send questions for panelists to safeguardsworkshop2020@ftc.gov

- To submit comments after the workshop go to www.regulations.gov

BREAK

Return at 9:30 AM

The Costs and Benefits of Information Security Programs

Panel Discussion:
Chris Cronin, Serge Jorgensen,
Pablo Molina, Sam Rubin

Moderator:
David Lincicum

BREAK

Return at 10:45 AM

Information Security Programs and Smaller Businesses

Panel Discussion:
Rocio Baeza, James Crifasi,
Brian McManamon, Kiersten Todt, Lee Waters

Moderator:
Katherine McCarron

NADA COST STUDY: AVERAGE COST PER U.S. FRANCHISED DEALERSHIP

Proposed Change[i]	One-Time Up-Front Cost	Annual Cost
Proposed Paragraph (a) – Appointing a CISO to increase program accountability.	$27,500	$51,000
Proposed Paragraph (b) – Requiring that the Information Security Program Be Based on a Written Risk Assessment.	$26,500	$26,500
Proposed Paragraph (c) (2) – Required Data and Systems Inventory	$16,750	$10,250
Proposed Paragraph (c) (4) – Requirement to Encrypt Data at Rest and in Transit.	$9,000	$8,500
Proposed Paragraph (c) (5) – Requirement to Adopt Secure Development Practices	$9,000	$37,500
Proposed Paragraph (c) (6) – Required Multi-Factor Authentication	$33,750	$18,500
Proposed Paragraph (c) (7) – Requirement to include Audit Trails.	$30,000	$18,000
Proposed Paragraph (c) (8) – Requirement to Develop Secure Disposal Procedures	$30,000	$10,800
Proposed Paragraph (c) (9) – Required Adoption of Procedures for Change Management	$30,000	$2,000
Proposed Paragraph (c) (10) – Required Unauthorized Activity Monitoring	$20,000	$29,000
Proposed Paragraph (d) – Required Penetration Testing and Vulnerability Assessments	$20,125	$23,125
Proposed Paragraph (e) – Required Employee Training and Security Updates	$2,100	$14,875
Proposed Paragraph (f) – Required Periodic Assessment of Service Providers	$14,250	$11,250
Proposed Paragraph (h) – Required Incident Response Plan	$16,000	$6,625
Proposed Paragraph (i) – Required Written CISO report	$9,000	$9,000
Total Cost Incurred/ Dealership[ii]	**$293,975**	**$276,925**
Total Cost Incurred Across All Dealerships[iii,iv,v]	**$2,236,267,825**	**$2,106,568,475**

Estimated Costs of Proposed Changes

Based on initial research

Multifactor Authentication
- Smartcard or Fingerprint Readers - $50
- Smartcards - $10 each

Inhouse Option
- Chief Information Security Officer - $180,000 yr
- Cybersecurity Analyst - $76,000 yr

or

Outsource Option
- Cybersecurity Contractor - $120,000-$240,000

Penetration Testing
- Average cost is $4,800
- Quote from local Cybersecurity company
  - External test - $2,160
  - Internal Test - $7,360

Physical Security
- Construction - $215,000
- New or Upgraded Locks - $10,000-$20,000

Costs would vary based on dealership size, but smaller businesses will have even less room in their budget for these expenses. Initial upgrades would be enough to put most dealerships out of business.

Models for Complying to the Safeguards Rule Changes

Model	Description	Helpful Resources
In-House	An employee wears the “CISO hat” and builds the program with support from internal teams	• Certifications • Training • Advisory services
Outsource	The company engages a service provider to wear the “CISO hat” to manage the program	• Professional services • Security in a box solutions
Hybrid	An employee manages the program and outsources activities, as needed	• All of the above

**Advisory services from an experienced CISO*

Available Service Providers and Cost Range

Service Provider	Service Type	Cost Structure
Company A *(AppSec focused)*	Security in a box solution	• $199/month: Startup (diy + starting templates) • $499/month: Complete (above + features to manage) • $2,000/day/month: Assisted (above + hand holding)
Company B *(Managed cyber security services)*	MSSP	• $599/month: Startup Tier (<10 employees) • $1,199/month: SME Tier (11-25 employees) • Addt'l fee for larger organizations
Company C *(Payday lending experts)*	Professional services	• $5,000 flat fee: Security strategy and roadmap development • $15,000/month: Part-Time Virtual CISO services • Addt'l fee for Full-Time Support

TECH LOCK

SAMPLE PRICING

SMALL

$2k–$5k
Per Month

25 - 250

EndPoints

MEDIUM

$5k–$15k
Per Month

250 - 750

EndPoints

LARGE

$15k–$30k
Per Month

750 - 1000

EndPoints

X-LARGE

$30k–$50k
Per Month

1500 - 2500

EndPoints

Vulnerability & Patch Mgt	**EndPoint Detection & Response**	**Log/SIEM**
Integrated Security Assessment / Compliance Maintenance	**Firewall Mgt**	**24x7x365 Security Operations Monitoring**

TECH LOCK

MFA/2FA Pricing (Duo)

Duo Free

Free

Basic

Up to 10 Users

Duo MFA

$3 Per User
Per Month

Adds Security Policy Checks

Duo Access

$6 Per User
Per Month

Device Trust Checks

More Robust Policy enforcement

Duo Beyond

$9 Per User
Per Month

Robust Device Trust Checks

App Policy Enforcement

SSO for Internal Corporate Resources

https://duo.com/pricing

LUNCH

Return at 1:00 PM

Continuous Monitoring, Penetration, and Vulnerability Testing

Panel Discussion:
Thomas Dugas, Fredrick Lee,
Scott Wallace, Nicholas Weaver

Moderator:
Alex Iglesias

BREAK

Return at 2:15 PM

Accountability, Risk Management, and Governance of Information Security Programs

Panel Discussion:
Adrienne Allen, Michele Norin,
Karthik Rangarajan

Moderator:
Robin Wetherill

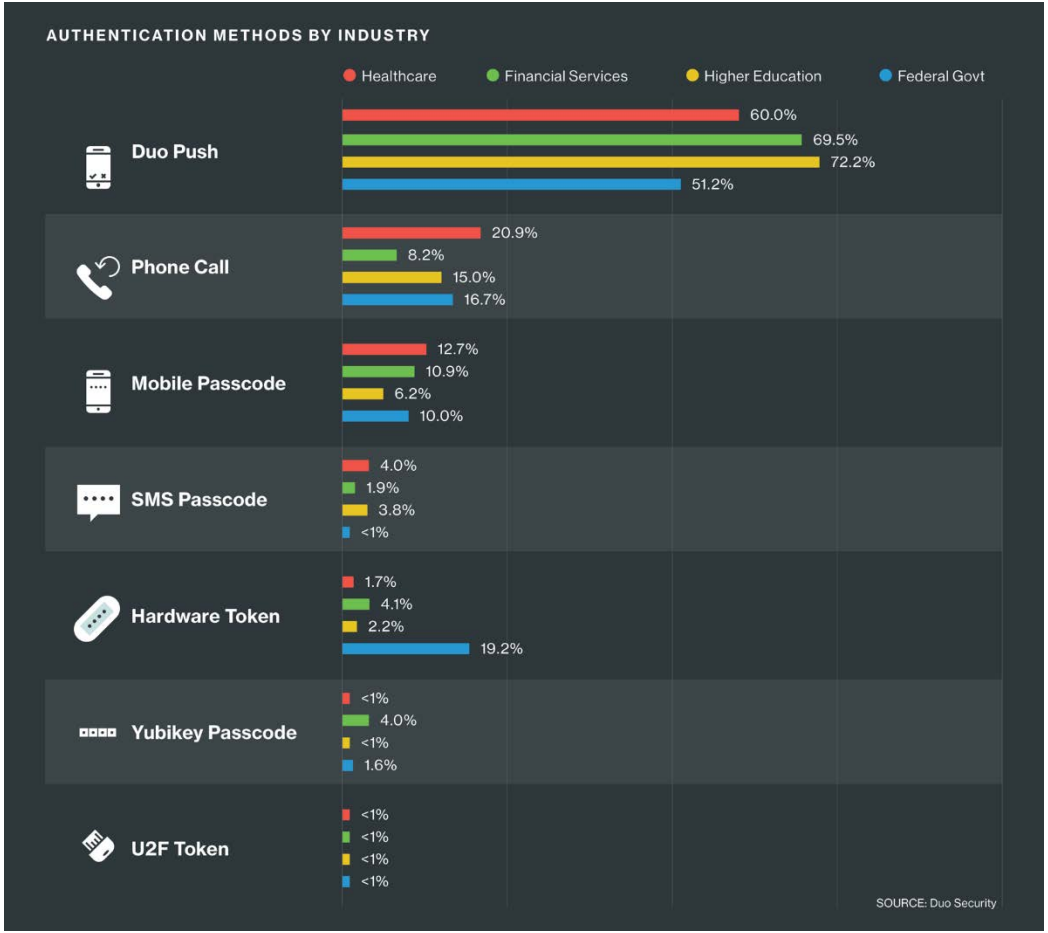
BREAK

Return at 3:30 PM

Encryption and Multifactor Authentication

Panel Discussion:
Matthew Green, Randy Marchany, Wendy Nather

Moderator:
Katherine McCarron


AUTHENTICATION METHODS BY INDUSTRY
Healthcare
Financial Services
Higher Education
Federal Govt
Duo Push
60.0%
69.5%
72.2%
51.2%
Phone Call
20.9%
8.2%
15.0%
16.7%
Mobile Passcode
12.7%
10.9%
6.2%
10.0%
SMS Passcode
4.0%
1.9%
3.8%
<1%
Hardware Token
1.7%
4.1%
2.2%
19.2%
Yubikey Passcode
<1%
4.0%
<1%
1.6%
U2F Token
<1%
<1%
<1%
<1%
SOURCE: Duo Security

Thank you for participating in the workshop!

Please submit your comments by August 12 to: www.regulations.gov