MORRISON | FOERSTER

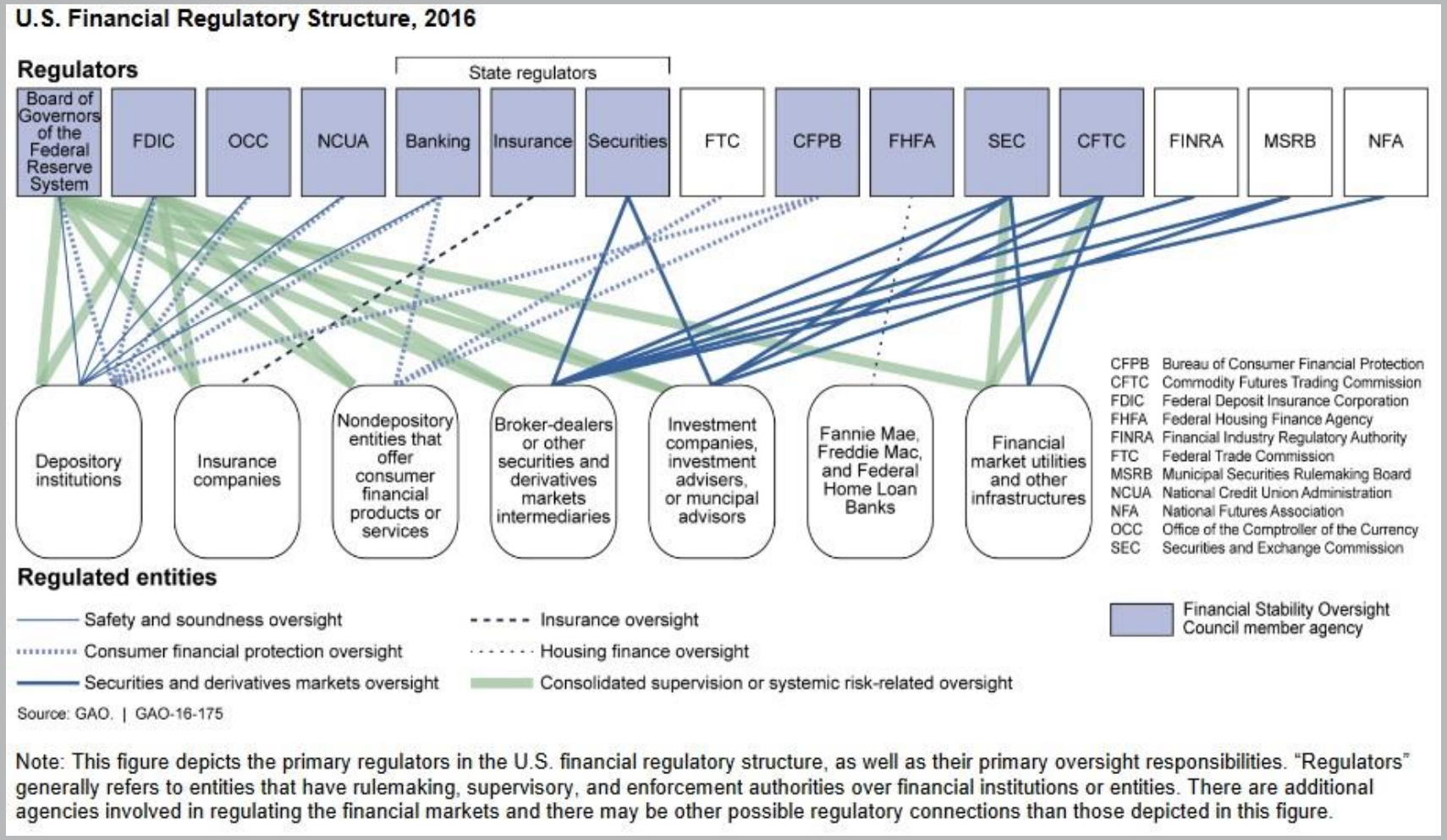
Cybersecurity and Data Protection Developments

Nathan Taylor

March 8, 2017

NY2 786488

Regulatory Themes



Note: This figure depicts the primary regulators in the U.S. financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure.

A "Developing" Regulatory Environment

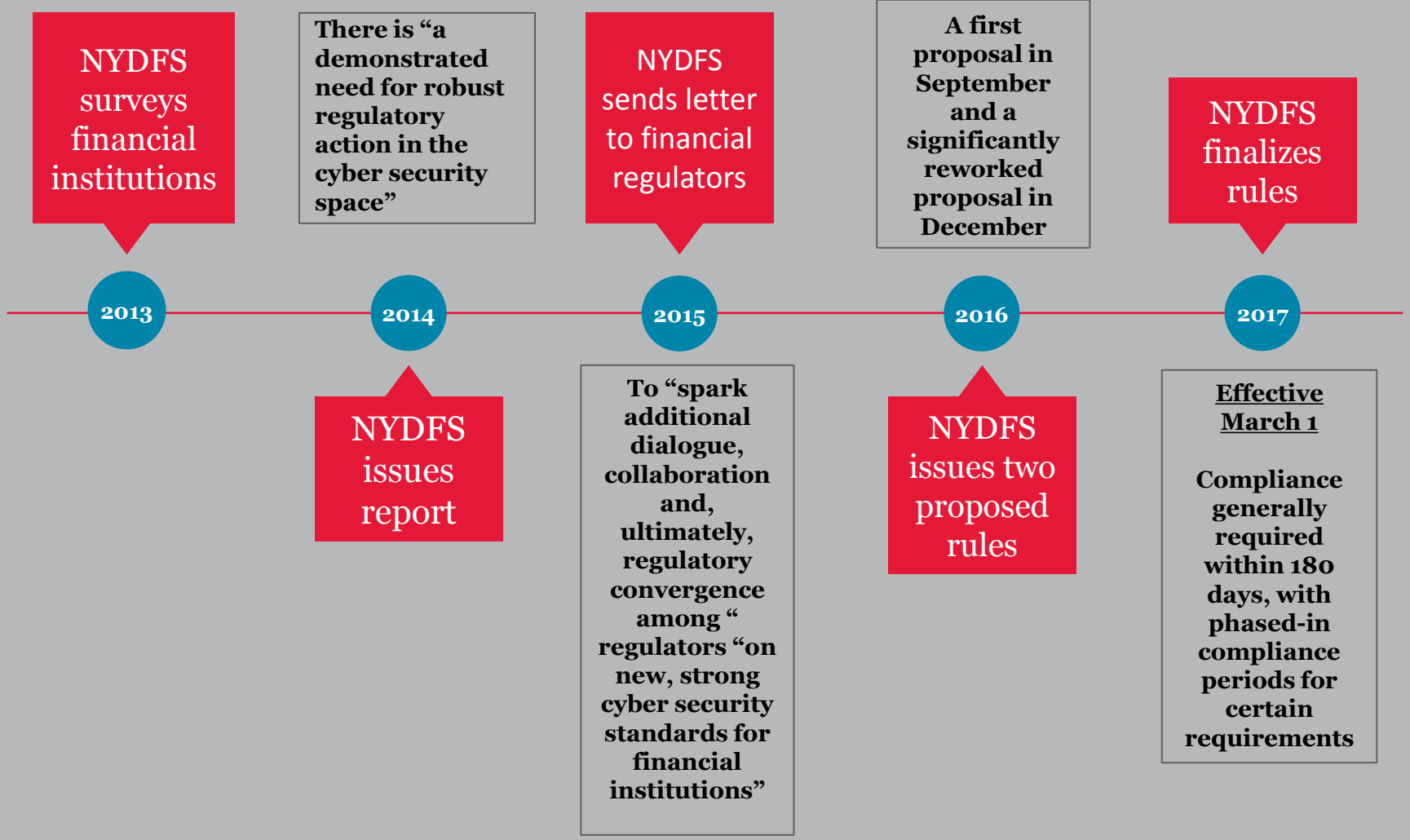
2016

- March – **CFPB** issues final Dwolla order
- September – **FFIEC** updates information security handbook
- October – **Banking agencies** issue enhanced cyber standard ANPR
- October – **FinCEN** issues cyber SAR advisory

2017

- February – **NYDFS** issues final cybersecurity rules

NYDFS – Background on Cyber Regs



NYDFS – Scope

Covered Entities

- Any person operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under NY banking, insurance or financial services law

Covered Information

- Business-related information that if compromised would cause a material adverse impact to the business, operations or security of the covered entity
- Information identifiable with consumers that includes certain sensitive data elements (*e.g.*, SSNs)
- Certain medical information

NYDFS – Requirements

Administrative Requirements

- Maintain a **cybersecurity program**
- Implement and maintain **written cybersecurity policies** addressing, for example, data governance, asset management, business continuity, system and network security and physical security
- Conduct periodic **risk assessments** to inform the design of the cybersecurity program
- Implement policies and procedures to address **application security**, **monitoring** user activity, and **data retention and deletion**
- Maintain a written **incident response plan**
- Maintain written policies and procedures relating to **third party service providers**
- Ensure that a **qualified individual** is responsible for overseeing and implementing the program
- Annual reporting to the Board of Directors on the state of the program
- Ensure **sufficient personnel** in place to oversee cybersecurity functions
- Regular **training** for all personnel on cybersecurity awareness

Specific Controls

- Conduct **penetration testing** and **vulnerability assessments**
- Maintain **audit trails**
- Limit user **access privileges**
- Implement **multifactor authentication**, including for access to internal networks from external networks
- **Encrypt** "nonpublic information" in transit and at rest

Notice

- 72-hour notice to DFS of certain types of security events

Reporting

- Annual certification of compliance with the regulations

Recordkeeping

- Maintain records supporting the annual certification
- Maintain systems that are designed to reconstruct material financial transactions sufficient to support normal operations

NYDFS – Requirements, cont'd.

NYDFS – Considerations

What does this mean?

How will NYDFS enforce? Like AML?

What will the federal financial regulators do (*e.g.*, the SEC)?

What will other states do (*e.g.*, Kentucky)?

Implications for Large FIs

Subsidiaries operating pursuant to a license or registration with NYDFS?

How will these rules impact transactions involving multiple FIs where one is regulated by NYDFS?

Banking Agencies – Cyber ANPR

Overview

- A framework for enhanced cyber risk management and resilience standards for certain "large and interconnected" financial institutions

Covered Entities

- Focus on financial institutions that the agencies believe are most critical to the country's financial system and economy
- Where a cyber event could impact the safety and soundness of the entity, other financial entities and the U.S. financial sector
- *E.g.*, holding companies and depository institutions with more than $50 billion in assets (and their subsidiaries) and financial market utilities (and their service providers)

Tiered Standards

- Enhanced standards to apply to all covered entities
- Higher standards for those entities "critical to the financial sector"

5 Categories of Enhanced Standards

To increase the covered entities' operational resilience and reduce the potential impact on the financial system as a result of, for example

- Cyber risk governance (*e.g.*, enterprise-wide cyber risk management strategy)
- Cyber risk management (in business units, an independent risk management function and audit)
- Internal dependency management for workforce, data, technology and facilities
- External dependency management of relationships with outside vendors, suppliers, customers and other third parties
- Incident response, cyber resilience and situational awareness

Sector-Critical Standards

- Require covered entities to substantially mitigate the risk of a disruption due to a cyber event to their sector-critical systems

CFPB – The Dwolla Consent Order

Allegations

- Dwolla made false representations to consumers regarding its data security
- "100% of [customer] info is encrypted and stored securely"
- All "sensitive information that exists on its servers" is encrypted
- Dwolla did not live up to its promises (*e.g.*, Dwolla did not use encryption)

Consent Order

- Based on UDAAP
- Dwolla deceived its customers because the representations that the company made were "likely to mislead a reasonable consumer"
- $100,000 civil money penalty

Takeaways

- CFPB (finally) makes move into the data security space
- Concern over FinTech "regulatory arbitrage"
- Implications for big banks?
- No public data security action since…

FFIEC – Continuing Guidance

Cyber Threat Sharing

- The sharing (and receipt) of cyber threat information between/among the private sector and the federal government "critical" to cybersecurity
- All financial institutions need "appropriate methods" to monitor, share and respond to cyber threat information
- Recommends that all financial institutions participate in the FS-ISAC

Cybersecurity Assessment Tool

- Intended to help financial institutions identify cyber risks and assess cyber preparedness (and determine whether they are aligned)
- Two parts: (1) a measure of inherent risk profile; and (2) a measure of cybersecurity maturity

IT Exam Handbook

- Revised in September 2016 to update examination expectations relating to an institution's culture, governance, information security program, security operations, and assurance processes

FinCEN – Cyber Advisory

The Advisory

- **Mandatory** – Cyber events intended to conduct, facilitate or affect a transaction or a series that involves or aggregates to $5,000 or more in funds or other assets
- **Voluntary** – Egregious, significant or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR (*e.g.*, a DDoS attach)

Nothing new here…

- FinCEN and the banking agencies have issued similar guidance in 1997, 2000 and 2005

Implications

- Push for cyber threat information (*e.g.*, IP addresses, indicators of compromise and device identifers)
- Frustration with the amount of cyber threat and intelligence shared with the federal government?
- Reminder of the need for communication among BSA/AML, cybersecurity, and other units of financial institutions
- Another example of the regulatory trend