MAYER·BROWN

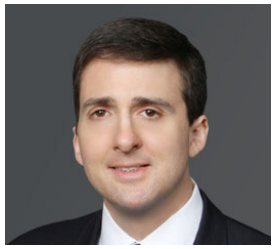
Trends in Data Breach and Cybersecurity Regulation, Legislation and Litigation

Part I

March 20, 2014

Speakers

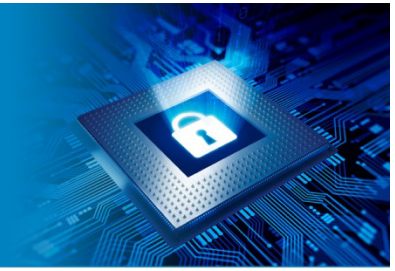
John J. Sullivan, Partner, rejoined Mayer Brown after serving as General Counsel at the US Department of Commerce in 2005 and then, following his nomination by President Bush and confirmation by the Senate, as Deputy Secretary until 2009. At Commerce, John was the senior official responsible for the Department's cyber security and worked closely with NSA to address threats posed by foreign governments and transnational criminal/terrorist organizations. From 2003 to 2005, he served as Deputy General Counsel of the Department of Defense, where he was the senior lawyer responsible for all of the Department's litigation, including its most sensitive national security cases. He is a former law clerk for Judge John Minor Wisdom and Supreme Court Justice David H. Souter.



Howard Waltzman, Partner, is a partner in our Government Relations practice in the Washington, DC office. Howard focuses his practice on communications and Internet law and privacy compliance. He represents some of the nation's leading communications service providers, manufacturers and trade associations in regulatory, compliance and legislative matters, including with respect to Internet and wireless services, privacy, video programming and cyber security.

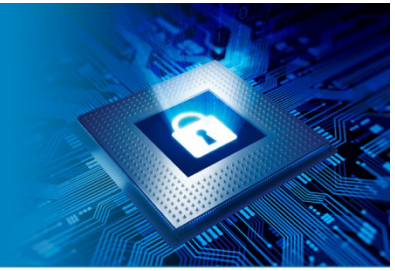
Stephen Lilley, Associate, is a Litigation & Dispute Resolution associate in Mayer Brown's Washington DC office and a member of the firm's Supreme Court & Appellate practice. He joined the firm in 2013, having previously worked for the Senate Judiciary Committee as Chief Counsel to the Subcommittee on Crime and Terrorism, and as Chief Counsel to the Subcommittee on Administrative Oversight and the Courts.

Agenda



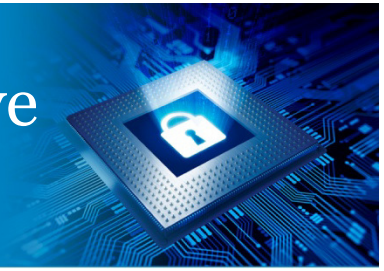
A. Data Breach
   - Contemplated legislative responses
   - Possible regulatory responses
   - Preview of April 17th webinar on data breach litigation

B. The NIST Framework for Cybersecurity
   - The origin, purpose, and content of the Framework v. 1.0
   - Considerations for companies
     - The "leverage" the Framework seeks to exert
     - Possible regulatory actions
     - Implications for possible litigation



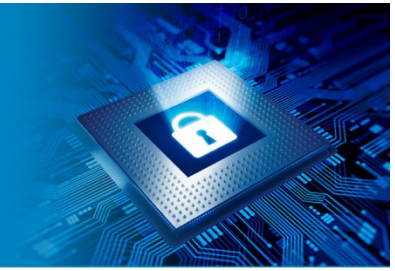
PART A – Data Breach

There Has Been Renewed Interest in a Legislative Response to Data Breaches



- Congressional interest in data breach notification and data security legislation has been renewed by recent high profile breaches
  - The Target and Neiman Marcus breaches have garnered particular attention
  - Other recent victims have included banks, startups, colleges, hospitals, and grocery stores
- Policymakers seek to protect privacy and enhance security
- Disagreement over how to achieve these goals has been sharp

The Legislative Debate Presents a Series of Significant Policy Questions



How prescriptive should data security standards be?

Should such standards be established through regulations?

What entities should be covered by new requirements?

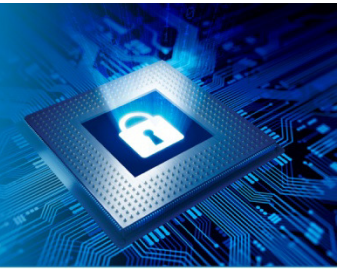
To what extent should state law be preempted?

Should the law provide a private right of action?

Should the FTC have primary, exclusive, or shared jurisdiction?

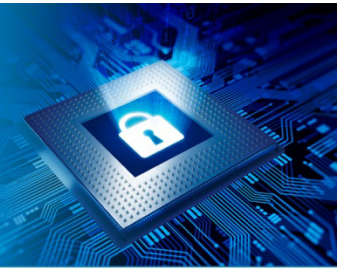
What role should state attorneys general and state enforcement agencies have in enforcement of the law?

There Are Indications That the House Energy and Commerce Committee May Consider Legislation



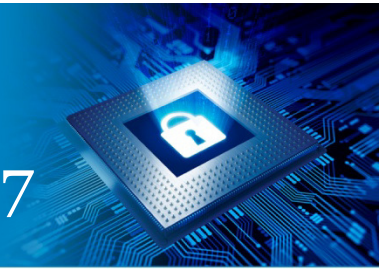
- Representative Lee Terry (NE-2) held a hearing on February 5th, 2014 to consider recent data breaches
  - Rep. Terry chairs the Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade
  - At the hearing, Rep. Terry explained that he opposes "codifying detailed, technical standards or . . . overly cumbersome mandates" and seeks to facilitate private sector "[f]lexibility, quickness and nimbleness"
- Representative Terry also has indicated interest in exploring legislation on this topic

Senate Legislation: The Toomey-King Bill, S. 1193



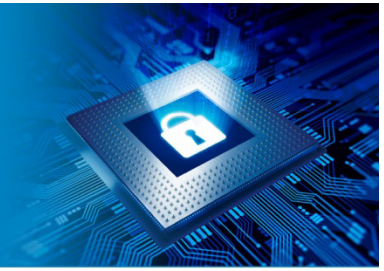
- There are a number of bills that have been introduced in the Senate
- The Toomey-King legislation would:
  - Require entities within the FTC's § 5 jurisdiction and common carriers subject to the FCC, see § 4(a)(1)-(2), to protect data pursuant to a "reasonableness" standard, § 2
  - Require those covered entities to notify affected individuals if the entity reasonably believes that a breach has caused or will cause financial harm, § 3(a)(1)
  - Be self-executing and not require rulemaking

Senate Legislation: The Carper-Blunt Bill, S. 1927



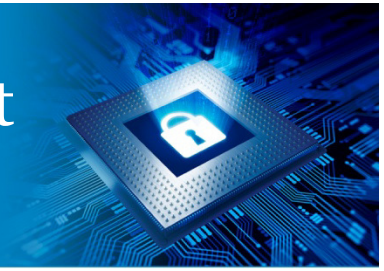
- The bill focuses on financial institutions, but covers any entity that "maintains or communicates sensitive account information or sensitive personal information," § 2(7)(a)
- The Carper-Blunt bill is before the Banking Committee. It would:
  - Require "reasonable" data security practices, § 3(a)(1), and notification to consumers if a breach is "reasonably likely" to cause "substantial harm or inconvenience" to consumers, § 3(c)
  - Require financial regulators (e.g. OCC, FDIC, etc.) and the FTC to issue implementing regulations as to entities within their enforcement jurisdiction, §§ 4-5

Senate Legislation: The Rockefeller bill, S. 1976, and the Leahy bill, S. 1897



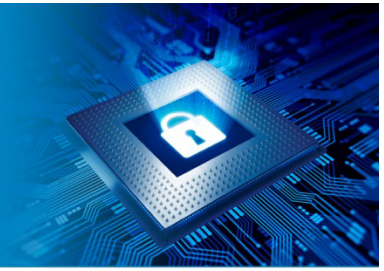
- The Chairmen of the Senate Commerce and Judiciary Committees have also introduced data security legislation
- The two bills are similar in many respects and differ primarily as to the roles of the FTC and the Justice Department. Each bill would:
  - Establish stringent new data security standards (the Rockefeller bill through FTC regulation, the Leahy bill by statute and regulation)
  - Require notification after a breach, even absent likely harm
  - Allow enforcement by state attorneys general

Regulatory Enforcement is Poised to Continue at Both the State and Federal Levels



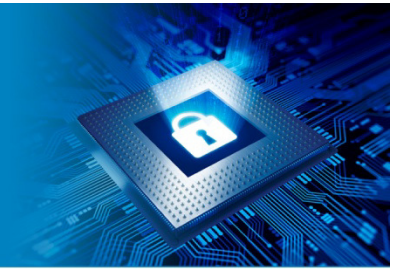
- The FTC continues to attempt to police data security practices through enforcement actions
  - The Wyndham and LabMD actions will determine the scope of the FTC's data security authority going forward
- As demonstrated in California, state regulators also are likely to continue to be active
  - California AG Kamala Harris has announced the prioritization of data breach investigations
  - California's breach notification requirement recently was expanded to be triggered by breach of "a user name or email address, in combination with a password or security question and answer that would permit access to an online account"

Data Breach Litigation Continues to Evolve and Expand in Significant Ways



The upcoming second part of this webinar, on April 17th, 2014, will consider issues including:

- Developments in data breach litigation
- New data breach and notification laws
- Enforcement efforts by state attorneys general
- Measures to prevent and defend against data breach lawsuits

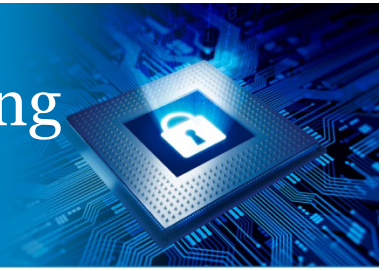


PART B: The NIST Cybersecurity Framework v. 1.0 – Legal and Regulatory Implications

The NIST Framework Has Its Roots in the Failed 2012 Effort to Pass Comprehensive Cybersecurity Legislation

- In the summer of 2012, Congress considered cyber threats to critical infrastructure:
  - The Senate considered legislation that would have allowed the creation, through regulation, of mandatory cybersecurity standards for critical infrastructure
  - When this approach stalled, a compromise was considered under which incentives, including liability protections, would be given in exchange for adoption of new voluntary cybersecurity standards
- After the legislation failed, President Obama issued Executive Order 13636, which ordered the creation of the NIST Framework

EO 13636 Included Four Key Directives Regarding the NIST Framework



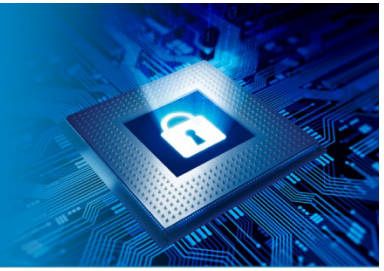
The National Institute of Standards and Technology (NIST) was tasked with creating the Cybersecurity Framework

The Department of Homeland Security was tasked with creating a voluntary program to support adoption of the Framework

A number of agencies were tasked with evaluating which incentives – including liability protections – would properly support adoption of the Framework

Regulatory agencies were required (or urged, in the case of independent agencies) to consider whether to act in response to the Framework

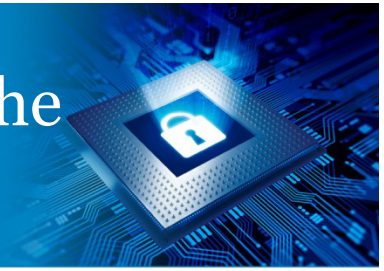
Like the Executive Order, the NIST Framework Focuses on Critical Infrastructure



- "Critical Infrastructure" is defined in the Executive Order and the Framework as:

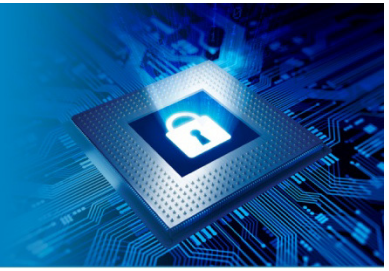
> "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

The NIST Framework v. 1.0 Is Consistent With the Principles Behind the Executive Order



- The Framework is based on **industry expertise and best practices** and ultimately is intended to be administered outside the government
- Adoption of the Framework and participation in the DHS program is **voluntary**
- The Framework reflects a **risk-based** approach to cybersecurity:
  - It is *not* one-size-fits-all
  - It is *not* a checklist
  - It is *not* technology specific

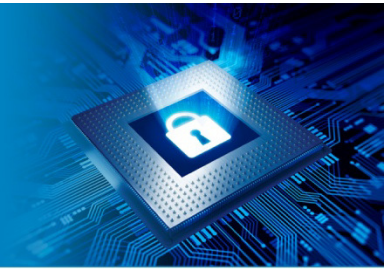
Framework Element One: the Framework Core



- The Framework Core "presents cybersecurity outcomes identified as helpful in managing cybersecurity risk"
- The Framework Core is broken into four elements:

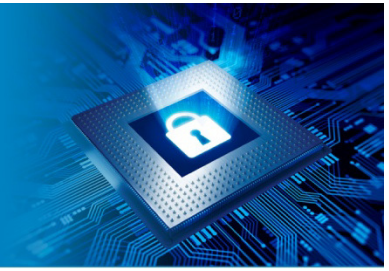
FUNCTIONS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
• The most general description of security activities • e.g. "Detect," "Respond"	• Provide the elements of the basic functions • e.g. "Asset Management," "Access Control"	• Divide categories into specific technical outcomes • e.g. "Data-at-rest is protected"	• Specific standards, guidelines, and practices associated with each subcategory

Framework Element Two: the Framework Implementation Tiers



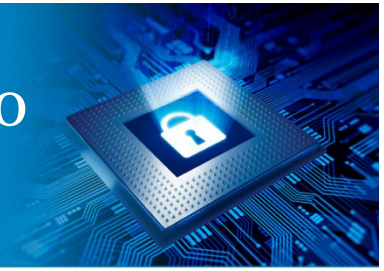
- The Framework Implementation Tiers provide entities with a means to categorize their overall cybersecurity performance
- The four Framework Implementation Tiers are “Partial,” “Risk Informed,” “Repeatable,” and “Adaptive”
- Each tier is expressed in terms of “Risk Management Process,” “Integrated Risk Management Program,” and “External Participation”
- “Tiers do not represent maturity levels,” so a company’s tier alone is not a measure of cybersecurity success

Framework Element Three: the Framework Profiles



- NIST describes a Framework Profile as "the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization"
- NIST also explains that an entity may generate a "Current Profile" and a "Target Profile"
- In other words, Framework Profiles are the products of a company's analysis of their current posture and their goals

Companies Now Must Decide How to Respond to the Framework

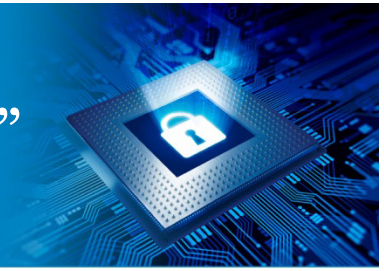


- Companies should make informed business decisions about their cybersecurity – this is not just a technical issue
- Key considerations include:
  - The "leverage" the Framework is intended to exert on industry
  - Possible regulatory activity based on the Framework
  - Possible efforts to use the Framework in litigation
- Critical infrastructure companies are most directly affected, but other companies also will be wise to consider the implications of the Framework

The NIST Framework Has Always Been Intended to Shift Private Sector Behavior Through "Leverage"

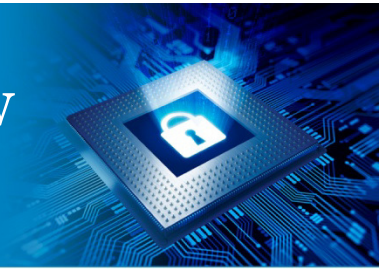
- Neither EO 13636 nor the NIST Framework attempt to shift industry behavior through civil liability
- However, the Framework, by creating a common "vocabulary," is intended to:
  - Support the development of private cybersecurity insurance markets
  - Facilitate the use of cybersecurity standards in vendor and service provider contracts
  - Close the gap between the CEO and the CISO regarding knowledge and appreciation of cybersecurity risks

Driving Improved Cybersecurity Through An Expanding Insurance Market Has Been a "Lever" of Particular Focus



- The Department of Homeland Security has held multiple stakeholder events on ways to support this market
- The basic theory has been that insurance companies will drive insured companies to maintain appropriate, risk-based practices
- The growth trajectory in this market remains uncertain, but anecdotal evidence is beginning to emerge that some insurance companies are working with their clients to strengthen cybersecurity

EO 13636 Directs Regulatory Agencies to Review and Respond to the Framework

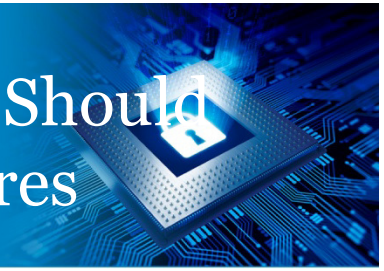


- The EO requires relevant regulatory agencies to consider "prioritized, risk-based, efficient, and coordinated actions … to mitigate cyber risk," § 10(a)-(b), and independent agencies are encouraged to take similar steps, § 10(e)
- Regulators should refrain from any effort to turn this voluntary program into a mandatory one:
  - Standards were not designed as mandates
  - Program should be given time to function as intended
- Companies should continue to educate their regulators about risk-based cybersecurity practices, improvements for the Framework, and the risks of mandatory regulation

The SEC Will Be Particularly Worth Watching, Since It Already Has Engaged On Cybersecurity Issues

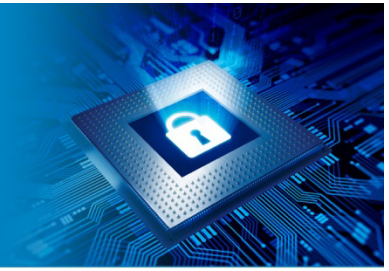
- In October 2011, SEC staff issued guidance about disclosures relating to cybersecurity
  - The SEC staff explained that registrants should review the adequacy of disclosure of "cybersecurity risks and cyber incidents"
- Since the issuance of the 2011 guidance, the SEC has questioned companies about their cyber risk disclosures
  - The SEC has issued at least 50 comment letters regarding cyber disclosures and companies have been forced to amend filings
- The SEC will hold a cybersecurity roundtable on 3/26/14

Until The SEC Speaks More Clearly, Registrants Should Consider if the Framework Can Inform Disclosures



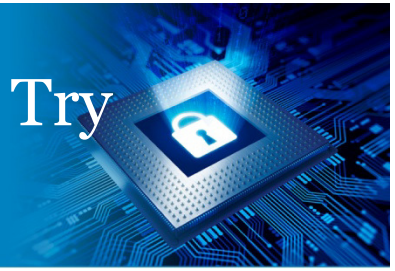
- The Framework is intended to provide a "common vocabulary" to communicate cybersecurity posture
- Registrants – and particularly owners and operators of critical infrastructure – should consider whether this "common vocabulary" actually will be helpful in disclosing the cyber risks
- Considerations will include:
  - How broadly the Framework has been adopted in a sector and used in disclosures by registrants in that sector; and
  - Whether the Framework is helpful to disclose the particular cyber risks facing the registrant

Financial Regulators May Issue New Industry Guidance Based On the Framework



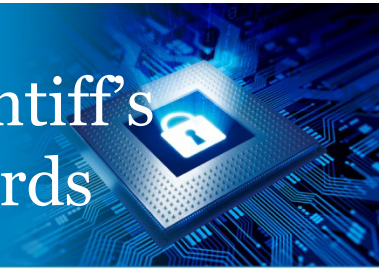
- Last June, the interagency Federal Financial Institutions Examination Council established a cybersecurity working group to "further promote coordination" on cybersecurity
- OCC head Thomas Curry testified this February that the FFIEC was "exploring additional approaches bank regulators can take to ensure that institutions of all sizes have the ability to safeguard their systems"
- Any resulting guidance is likely, at a minimum, to inform supervisory examinations going forward

A Range Of Regulators Also May Be Tempted to Try to Use the Framework in Enforcement Actions



- The FTC has not indicated whether it sees a role for the Framework in data breach litigation
- The CFPB has taken an exceptionally broad view of its jurisdiction and its vague and expansive authorities
  - To date, the CFPB has not engaged on cybersecurity issues
  - Notably, the CFPB can bring enforcement actions for "abusive" practices that, *inter alia*, "take unreasonable advantage of … the reasonable reliance by the consumer on a covered person to act in the interests of the consumer," 12 U.S.C. § 5531(d)(2)

Companies Should Fight Any Efforts By the Plaintiff's Bar to Turn the Framework Into Binding Standards



- Attempts to transform elements of the Framework – and particularly the Framework Core – into binding legal standards, whether in negligence actions or other suits, would be contrary to the purposes of the EO and the NIST Framework
- Such efforts should be strongly resisted since they:
  - Would reduce stakeholder interest in collaborating on consensus standards
  - Are inconsistent with risk-based cybersecurity practices
  - Would harm cybersecurity since the success of such actions would create static and immediately obsolete standards

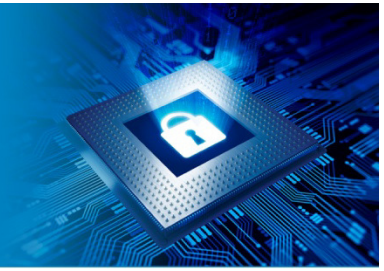
Companies Also Should Anticipate Securities Class Actions Seeking to Make Use Of the Framework

- Observers have recognized the possibility that the plaintiff's bar may press securities litigation alleging material omissions or misrepresentations about cyber risks
- Given that such lawsuits may be inevitable, businesses that own or operate critical infrastructure will want to take account of the Framework in evaluating and disclosing cyber risks
- Other registrants also will want to consider whether they can insulate themselves from securities litigation through the principles underlying the Framework

Companies Also Should Consider the Possibility of Actions Against Directors and Officers That Reference the Framework

- Derivative actions that allege breach of the duty of care or breach of the duty of loyalty may be raised
- Evaluating and managing cybersecurity against the Framework, or comparable risk-based practices should trigger the protections of the business judgment rule
  - E.g., In re Citigroup Inc. Derivative Litig., 964 A.2d 106, 123-24 (Del. Ch. 2009)
- As other commentators also have suggested, the duty of loyalty may be implicated if plaintiffs allege the "unconsidered failure of the board to act"
  - *Id.* at 122-23

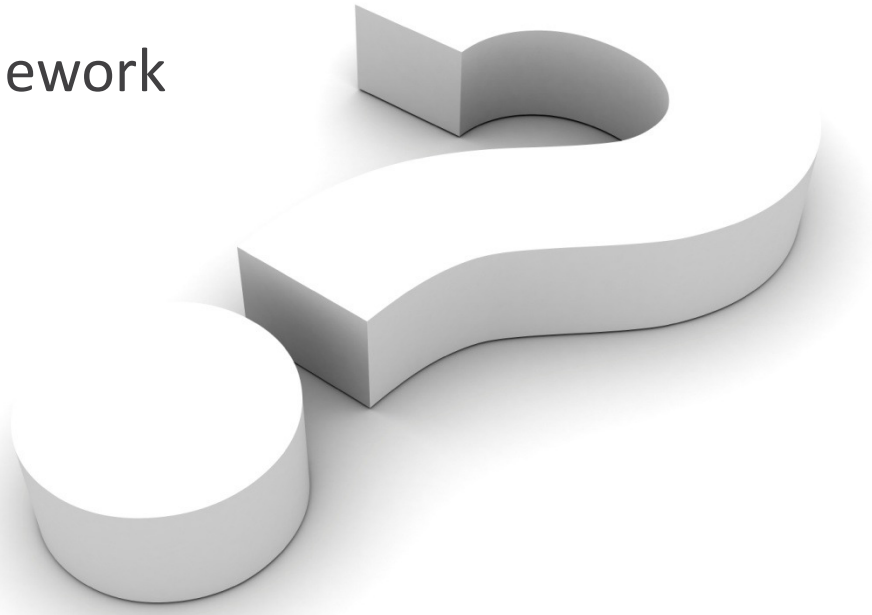
Case Law Under UCC Article 4A May Also Be Informed By the Framework Going Forward



- UCC Article 4A governs liabilities for commercial funds transfers, and limits liabilities for banks with "commercially reasonable" security procedures
- In *Patco Construction Company, Inc. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012), the Court found the "one size fits all" cybersecurity of a community bank not "commercially reasonable"
- Although every bank will not qualify as "critical infrastructure," use of the Framework may help banks ensure "commercial reasonableness" after *Patco*

Wrap-Up and Questions

- Data breach
- Cybersecurity and the NIST Framework
- Further considerations
- Questions?



John J. Sullivan
Partner
+1 202 263 3004
jjsullivan@mayerbrown.com

Howard W. Waltzman
Partner
+1 202 263 3848
hwaltzman@mayerbrown.com

Stephen Lilley
Associate
+1 202 263 3865
slilley@mayerbrown.com

MAYER·BROWN