The Compliance Role in Information Security & Cyber Security

Don Griffith
Head of Financial Crimes & Fraud Prevention Compliance
MassMutual

Matt Kelly
Editor & CEO
Radical Compliance

SCCE Boston Conference
29 March 2019

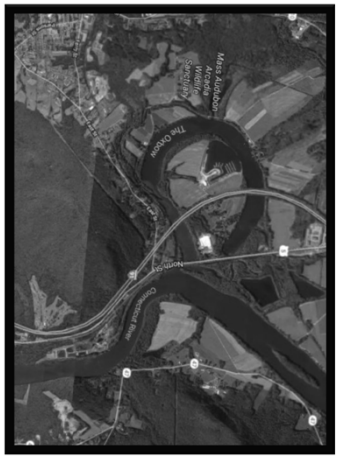
Agenda

- The evolving regulatory landscape
- Regulators' expectations of the compliance role in cybersecurity
- Assessing the compliance risks relating to information security
- Leveraging your internal experts
- The intersection of information security, privacy, anti-money laundering, and fraud compliance

THE EVOLVING REGULATORY LANDSCAPE

Thomas Cole, *The Oxbow, View from Mount Holyoke, Northampton, Massachusetts, after a Thunderstorm* (1836), Metropolitan Museum of Art

- Not only is the landscape changing; also the tools we use to describe it
- Focus on privacy and personal information shifts from one of **consumer protection** to a **human right**
- Emphasis is on greater personal control over information others (particularly companies) possess about the individual
- Coupled with increased regulatory requirements on access and protection (i.e., security) of personal information and assets entrusted to a company



Google Maps, "Satellite" mode, March 2019.

THE EVOLVING REGULATORY LANDSCAPE

- At least 35 states, D.C. and Puerto Rico introduced or considered more than 265 bills or resolutions related to cybersecurity. Key areas of legislative activity include:
- Improving government security practices.
- Providing funding for cybersecurity programs and initiatives.
- Restricting public disclosure of sensitive government cybersecurity information.
- Promoting workforce, training, economic development.
- At least 22 states enacted nearly 60 bills in 2018

Source: National Conference of State Legislators, "Cybersecurity Legislation 2018" http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

EU General Data Protection Regulation (GDPR)

- So important it has its own Wikipedia page!
- Organizations within EU, or any organization outside EU that offer goods or services to, or monitor the behavior of, EU data subjects.
- **Gives individuals greater control over their personal data** and imposes significant obligations on organizations that collect, handle or analyze personal data.
- **Transparency in handling and use of personal data.** Be clear with individuals about how you are using personal data and **need a lawful basis' to process that data**.
- **Limits processing of personal data** to specified, explicit, legitimate purposes. No re-use of personal data for purposes not 'compatible' with the purpose for original collection.
- **Ensures accuracy of personal data.** You will need to take steps to ensure that personal data you hold is accurate and can be corrected if errors occur.
- **Limits storage of personal data.** Retain personal data only for as long as necessary to achieve the purposes for which the data was collected.

NY Department of Financial Services Cybersecurity Rule

Financial firms over certain size, doing business within state of New York, must establish cybersecurity program that includes…

- Asset inventory and device management,
- Access controls,
- Disaster recovery plans,
- Vendor and third-party service provider management,
- Written Incident Response Plan;
- Written Cybersecurity Policy;
- Designate a Chief Information Security Officer (CISO) responsible for cybersecurity program and policy;
- Reporting certain cybersecurity events to the DFS within 72 hours, submitting annual compliance certifications to the DFS by February 15 of each year.

California Consumer Privacy Act

- Requirements go into effect 1 Jan. 2020
- Applies to for-profit entities
  - Gross revenue in excess of $25 million
  - Receive/share personal information of more than 50,000 consumers, or
  - Derives at least half annual revenue by selling personal information of California residents
- Broad definition of personal information
- Right to know what personal information a business has collected about the resident
- Right to opt of business selling personal information to 3rd parties
- Right to have information deleted
- Right to receive equal service and pricing even if resident exercises privacy rights under the act
- Fines up to $7,500 per violation
- Private right of action with minimum of actual damages of between $100-$750 per incident

Regulators' expectations of compliance and cybersecurity

- Convergence of regulatory interest across privacy, cybersecurity and consumer protection
- Regulators expect compliance to be part of the equation
- Compliance professionals will need to keep up

Securities & Exchange Commission

- **Guidance on Public Company Disclosures:** 'cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws.'
- **Revived SEC Cyber Unit:** cryptocurrencies, cybersecurity controls, issuer disclosures, trading based on hacked information, market manipulation via social media, etc.
- **Safeguards Rule and Identity Theft Red Flags Rule** enforcement
- Warning against business email exploits

FINRA

- Will also continue to review adequacy of firms' cybersecurity programs to protect sensitive information;
- Recently published Report on Selected Cybersecurity Practices – 2018; provides additional information on practices that may help some firms strengthen their cybersecurity programs.

Defense Department

- DFARS compliance for government contractors: effective 1 Jan. 2018
- Ensure NIST cybersecurity standards extend to contractor's third parties

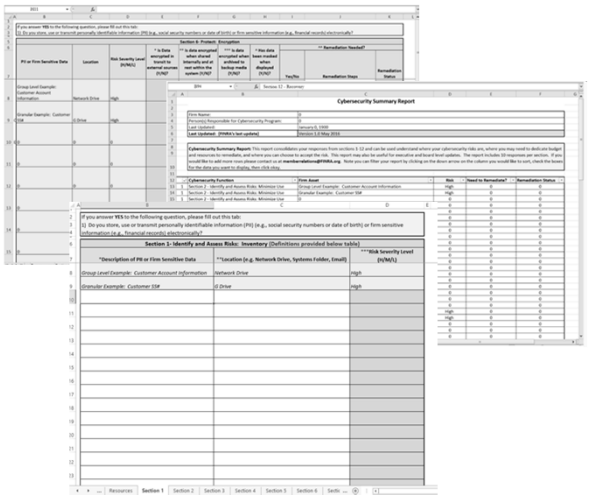
Assessing compliance risks relating to information security

- Compliance risk assessment
- FAIR methodology (Factor Analysis of Information Risk)
- Leverage CISO/IRM risk assessments
- Consider starting simply
  - Inherent risk (probability, impact, speed of onset)
  - Summary control assessment
  - Residual Risk
    - Proposed mitigations

Assessing compliance risks relating to information security

- FINRA provides useful tools for performing a cybersecurity risk assessment
- Use it to
  - identify and assess cybersecurity threats, protect assets from cyber intrusions
  - detect when their systems and assets have been compromised
  - plan for the response when a compromise occurs
  - implement a plan to recover lost, stolen or unavailable assets

Source: http://www.finra.org/industry/small-firm-cybersecurity-checklist



Assessing compliance risks relating to information security

Third parties: Yes, panic

From Ponemon Institute report, Sept. 2018:

- 29 percent say a third party would contact them about the data breach;
- 37 percent say they have sufficient resources to manage third-party relationships;
- 35 percent rate their third-party risk management program as highly effective;
- 57 percent do not know if their organizations' vendor safeguards are sufficient to prevent a breach.
- **34 percent say they have a comprehensive inventory of all their third parties.**

Survey of more than 1,000 security professionals in U.S., U.K.

Leveraging your internal experts

- IT
- Risk Management, Information Risk Management
  - CISO
  - FAIR methodology
- Data Analysts
- Existing committees (Risk, GRC, Fraud, Information Security, others?)
- Communication, Coordination

Policy and procedure considerations

- Which employees might handle inquiries from consumers?
  - Do they know what to do?
  - Do they know when to say no?
- You want to try a self-service approach…
  - Does the firm have a single source of all PII data?
  - Does the system know when to say no?
- Someone wants to collect new types of PII…
  - Has that been reviewed by data protection officer?
  - Do training materials clearly, strongly explain the policy?

Q&A

Thank you Boston!

The intersection of information security, privacy, anti-money laundering and fraud compliance

Delineating responsibilities

- Consider who owns:
  - Governance and risk management
  - Information Security Tools
  - System change management
  - Policies
  - Standards
  - Procedures
  - Controls (Technical, regulatory, other)
  - Incident response planning/execution
  - Data loss prevention
  - Regulatory Reporting
  - Management/Board reporting, KPIs
  - Oversight/Monitoring
  - Training/education
  - Cyber intelligence/Information sharing
  - Vendor due diligence
  - Risk Assessment, KRIs

"Cybersecurity, anti-fraud and AML programs often have common elements and controls, as well as synergies across people, processes and technology. Most firms are going to find that certain processes should be combined and others should remain separate but share Information more closely."

--*Building a united front on financial crimes*, PWC, October 2018.

The intersection of information security, privacy, anti-money laundering and fraud compliance

The Environment: An Emerging Trend

- Financial institutions are rethinking their organizational structures to manage financial crime risk more effectively
  - Driving greater coordination among the three lines of defense and requiring each line, in turn, to develop more integrated, robust approaches
  - Alignment of business, risk, compliance, and audit functions will be crucial if the financial services sector is to address the broader sources of financial crime risk and tightening regulation
- Companies are exposed to increasingly sophisticated techniques used by fraudsters and other criminals, who target new vulnerabilities as large volumes of customers perform multiple transactions across multiple channels
  - Cyber threats are only one part
  - Companies are grappling with fraudsters and other criminals who often target (in a coordinated fashion) a number of different internal and external channels
- Regulatory burden is increasing, including greater customer protection, monitoring customer activity (AML, elder abuse/reporting), privacy, cybersecurity, sanctions and watch-lists
- Significant compliance burden as regulation continues to tighten, and as customers and other stakeholders demand greater transparency and integrity in financial dealings.

"More than ever before, financial institutions are challenged to meet financial crimes compliance obligations in a more cost-effective way…Many financial institutions are addressing this by integrating their existing anti-money laundering, sanctions, fraud, surveillance and anti-bribery and corruption compliance programs under a unified financial crimes umbrella."*

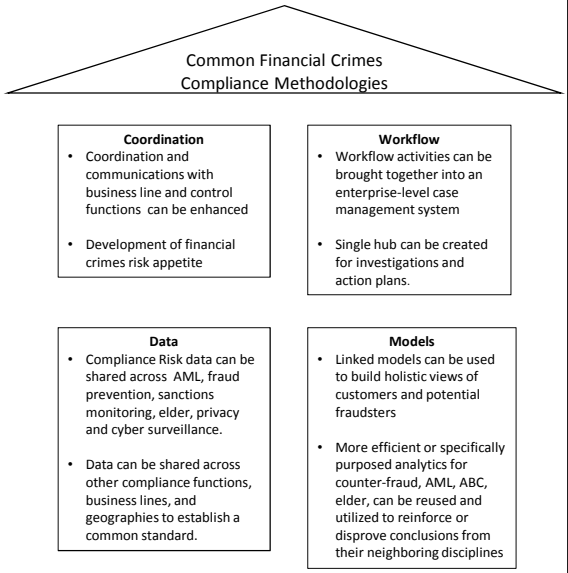
**Under One Agile Umbrella: An Approach to Managing Financial Crimes Risk*, KPMG, 2017.

18

The intersection of information security, privacy, anti-money laundering and fraud compliance

A key issue to be addressed could be an opportunity:

- The need to align various compliance efforts taken to manage financial crime risk and compliance across the organization.
  - For example, some aspects of financial crimes compliance, such as counter-measures for internal and external fraud, are directly driven by the business case and introduced to prevent direct losses.
  - Other aspects are driven by regulation, such as AML, elder financial exploitation, anti-corruption, FATCA, and sanctions monitoring, and by indirect losses in the form of regulatory fines and brand erosion.
- The risk is that these different motivations for change may lead to change processes being undertaken by isolated teams that are not working toward the aligned compliance risk appetite of the firm.
- Ideally, these individual initiatives need to be managed as a portfolio with a ***vision for an integrated target operating model—a Financial Crimes Compliance unit.***



*For more information, see http://www.ey.com/Publication/vwLUAssets/ey-tackling-financial-crime-through-integrated-risk-and-compliance/$FILE/ey-tackling-financial-crime-through-integrated-risk-and-compliance.pdf

19

The intersection of information security, privacy, anti-money laundering and fraud compliance

The Potential Benefits and Pitfalls

- Alignment and integration regarding financial crimes prevention is still at a relatively early stage
- Greater focus on fraud prevention has led to increased alignment and coordination among the business (first line of defense) and control functions (Risk Management, Information Risk Management, Compliance & Ethics, Audit)
- A logical next step is to develop greater internal coordination/integration within the Compliance & Ethics Department

THE POTENTIAL BENEFITS

- Improved integration, coordination, and collaboration to manage financial crimes risk across the enterprise
- Expanded view of financial crimes risks and trends
- Heightened senior leadership awareness of risks and control environment
- Sharper focus on corporate compliance functions and efficiencies
- Added cost savings resulting from complexity and duplication
- Enhanced ability/agility to comply with changes to regulatory expectations
- Improved data aggregation and data analytics and enhanced technology infrastructure

THE POTENTIAL PITFALLS

- Potential for form over substance given current activities already in place if no plan for substantial enhancement is developed
- Reorganization can be disruptive and affect morale

20

Core Responsibilities for Financial Crimes & Fraud Prevention Compliance Unit

Financial Crimes Prevention Compliance

- Anti-fraud
- Anti-Money Laundering/BSA
- Information Governance/Privacy/Cybersecurity
- Anti-Corruption
  - Gifts/Entertainment
  - Conflicts of Interest
  - Political Contributions
  - Government Business RFP Review
- Economic Sanctions
- Elder & Vulnerable Adults
- Insider Trading
- Antitrust