A Special ACAMS Presentation
Tuesday, April 4 | 11:15 AM

Moderator:
John J. Byrne, Esq., CAMS, Executive Vice President, ACAMS

Speakers:
Susan J. Galli, CAMS, Managing Director, Advisory Financial Crimes Unit, PwC
Megan Davis Hodge, Executive Compliance Director, BSA/AML Officer, Ally Financial
Richard Weber, Chief Criminal Investigation, Internal Revenue Service (IRS)
Topics and Challenges

- The Convergence of Fraud, AML and Cyber in 2017
- The Dark Web
- IRS Criminal Investigations
- Third Party Due Diligence
- The Clearing House AML Report and Recommendations
- DOJ Guidance For Evaluating Corporate Compliance Programs
The Convergence of Fraud, Cyber and AML

Guidance to U.S. Financial Institutions explains how BSA regulations and requirements apply to cyber events, cyber-enabled crime and cyber-related information

I. Mandatory and Voluntary SAR Reporting of Cyber Events

II. Including Cyber-Related Information in SAR Reporting

III. Collaboration between BSA/AML and Cybersecurity Units

IV. Sharing Cyber-Related Information between Financial Institutions using 314(b)

For Immediate Assistance: Contact Regulatory and Law Enforcement Agencies and Voluntary SAR Reporting of Cyber Events

The Convergence of Fraud, Cyber and AML – NYDFS Part 500

- Last December, the NY State Department of Financial Services (“NYDFS”) issued a Proposed Regulation (Part 500) requiring, among other Things, prompt Reporting of Cybersecurity Incidents that are likely to have a Material Impact on the Business.
- Covered Institutions are required to have a Cyber-security Program with Policies and Procedures in place by August 28, 2017, overseen by a Chief Information Security Officer (“CISO”), and must certify as to Compliance by February 15, 2018.
- The Regulation also requires that the Cybersecurity Policy address 14 Specific Areas including, but not limited to Information Security, Data Governance and Classification, Customer Data Privacy and Risk Assessments.
- Similar to NYDFS Regulations published last Year on Watch List Filtering and Transaction Monitoring, Part 500 also requires that the Internal Controls be calibrated based on a Risk Assessment and include Things such as Penetration Tests and Vulnerability Assessments, Multi-Factor Authentication, Encryption of In-Transit and At-Rest Data, Auditing of Systems and Financial Transactions and Access Controls.
- Part 500 requires that an Organization report, within 72 hours, any Cyber Incident that is reasonably likely to materially impact the Operations of the Covered Financial Institution, and these will generally overlap with FinCEN’s SAR Requirements.

Source: www.newyorklawjournal.com/printerfriendly/id=1202780356588
The Dark Web

Surface Web:
- Google
- Bing
- Wikipedia

Deep Web:
- Academic Information
- Medical Records
- Legal Documents
- Scientific Reports
- Subscription Information
- Social Media
- Multilingual Databases
- Financial Records
- Government Resources
- Competitor Websites
- Organization-specific Repositories

Dark Web:
- Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.
- A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. **Deep Web Technologies has zero involvement with the Dark Web.**
- Illegal Information
- TOR-Encrypted sites
- Political Protests
- Drug Trafficking sites
- Private Communications
The Dark Web

- The Dark Web is a Collection of Websites that are Masterfully hidden from the General Public. Most of these Websites hide their IP Addresses which makes it impossible to identify Who is behind the Screen
The Dark Web

- The Dark Web is a Murky Place where you can buy Illegal Guns, Illegal Drugs, Fake Money, Fake IDs, and even arrange to have People killed, all with Total Anonymity.
IRS – Criminal Investigation

Our Cyber Initiative

- Connecting the Dots Thru the Power of Analytics - Combining multiple data sources - Device ID, IP addresses, Tax, FinCEN, Panama Papers, Swiss Bank Program data, etc.
- Identifying emerging threats – Cyber Response Team
- Online investigations nationwide focusing on darkweb activity
- Two Cyber Crimes Units – Washington, DC & Los Angeles, CA

Opportunities to Work Together

- Fighting cyber crime must be a collaborative process
- The IRS’ current efforts
  – Security Summit and ISAC partnerships
- NY Department of Financial Services – cybersecurity regulation (effective 3/1/17)
Third Party Due Diligence

• Compliance/AML risk should be considered as part of overall Vendor Management program
• You can outsource the function, but never the risk
• In today’s environment, view service providers as if they were your own employees
• Outsourcing general bank functions (contact center) versus AML-specific functions (alert review, etc)
• Look to general compliance enforcement actions related to vendors to gain insights on how the regulators view the issues
• Going beyond having the “right” covenants included in the contract...the importance of ongoing monitoring and supervision
• Any decision-making by a third party heightens risk
AML Report and Recommendations
(Excerpt)

- Assessment of the Existing Regime concluded that the current AML/CFT Statutory and Regulatory Framework is outdated and thus ill-suited for apprehending Criminals and countering Terrorism Threats in the 21st Century.

- Potential Reforms – Recommendations that would (i) make the AML/CFT Regime more effective as a Tool for Law Enforcement and National Security; and (ii) reduce the Collateral Damage imposed by the Current AML/CFT Regime—generally, needlessly—on other Important National Priorities such as the Projection of U.S. Influence Globally, the Alleviation of Poverty in Less Developed Countries, and the Availability of Banking Services in Underserved Communities in the United States.

- Areas for Immediate Reform – High Priority Reforms where there was a Clear Consensus on Both the Immediate Need for the Reforms and their Wisdom.

- Areas of Reform Requiring Further Study – Reforms warranting further Consideration, because Potential Solutions may involve Difficult Tradeoffs, or where Input from Other Stakeholders would be Beneficial.
U.S. Department of Justice (‘DOJ”) Criminal Division Fraud Section Evaluation of Corporate Compliance Programs (Excerpt)

- **Conduct at the Top** – How have Senior Leaders through their Words and Actions, Encouraged or Discouraged the Type of Misconduct in Question?

- **Shared Commitment** – What Specific Actions have Senior Leaders and other Stakeholders taken to demonstrate their Commitment to Compliance, including their Remediation Efforts?

- **Oversight** – What Compliance Expertise has been Available to the Board of Directors? Have the Board of Directors and/or External Auditors held Executive or Private Sessions with the Compliance and Control Functions? What Types of Information have the Board of Directors and Senior Management examined in their exercise of Oversight in the Area in which the Misconduct occurred?
Takeaways

- Immediately conduct a Gap Assessment between Existing Policies and Procedures around Incident Reporting and the FinCEN Advisory and Part 500 Requirements to develop an Action Plan to address Identified Gaps.

- Assess your Organization’s Structure to determine what Coordination and Cooperation may already exist between the Cybersecurity, Fraud and AML Compliance Functions to facilitate Coordinated Reporting to meet Applicable Regulatory Reporting Requirements related to Cyber Events.

- Understand where your Organization engages with Third Parties and assess risks and controls required from an AML standpoint—not just AML-related processes, but other general processes.
IRS – Criminal Investigation

Strategic Takeaways

- Is your reporting of suspicious activity comprehensive? Does it include the data collected by your cybersecurity or IT department?
- Does your organization have a reporting stream that alerts law enforcement immediately when suspicious activity is detected? Is FinCEN reporting the only way you alert law enforcement?
References


- See FinCEN Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs), (October 25, 2016) https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF

- See Department of Financial Services Frequently Asked Questions Regarding 23 NYCRR Part 500 http://www.dfs.ny.gov/about/cybersecurity_faqs.htm

- See “A Meeting of the Minds: Emerging Regulation and the Convergence of Cyber and Fraud” available at http://www.newyorklawjournal.com/printerfriendly/id=1202780356588


- See “Evaluation of Corporate Compliance Programs”, U.S. Department of Justice, Criminal Division, Fraud Section https://www.justice.gov/criminal-fraud/page/file/1937501/download
Questions
We want to hear from you!

Rating a Session

• Click on session
• Scroll down to the ‘Files & Links’
• Click on ‘Rate this Session’

Rating a Speaker

• Click on speaker
• Scroll down to ‘Rate and Review’
• Select number of stars
• Click to ‘Write a review’

Rate this session & speakers in the mobile app