Cyber-Enabled Crimes – Working with Your IT Partners

BSA Coalition Anti-Money Laundering Conference
June 6, 2017
The views and opinions expressed here are those of the speakers. They do not represent an official position of the Federal Reserve Bank of Richmond or the Federal Reserve System.
Moderator: Cara Mitchell, Managing Examiner, Supervision, Regulation and Credit, Richmond Fed
Panelist: Mark Hanson, Section Chief of Cyber and Emerging Technologies, Financial Crimes Enforcement Network
Panelist: Jeremy Kuester, Deputy Associate Director, Financial Crimes Enforcement Network
Panelist: Bryan Newlin, Audit Manager – Risk Advisory Services, Yount, Hyde & Barbour
Panel Topics

- FinCEN Advisories on cyber topics
- Types of cyber incidents
- Importance of communication between BSA/AML and IT
- SAR best practices for cyber incidents
- Reference materials
Takeways

- Incorporate the IT business line into your communication routines
- Make sure you are familiar with FinCEN Advisories on cyber topics
- If possible, report cyber incidents within 24 hours to law enforcement
- Follow best practices for reporting SARs on cyber incidents
Takeways - cont’d

When filing SARs on cyber incidents, include all pertinent information:

- Relevant e-mail addresses and associated Internet Protocol (IP) addresses with their respective timestamps
- Use FinCEN key terms like “BEC FRAUD” or “EAC FRAUD” in the case of business e-mail or e-mail compromise fraud
- The type, magnitude, and methodology of the cyber-event as well as signatures and facts on a network or system that indicate a cyber-event
Reference Materials

FIN 2016-A005 – Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crimes
FIN 2016-A003 – Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes
FAQ Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime and Cyber-Related Information through SARs
FIN 2014-A007 – Advisory to Financial Institutions on Promoting a Culture of Compliance
Questions?