Introductions

Our Moderator:

Greg Ruppert
Vice President
Financial Crimes Investigations
Charles Schwab

Our Panelists:

Chris Wallace
Lead Intelligence Analyst
CenturyLink

Tim Wallach
Supervisory Special Agent
Federal Bureau of Investigation

Ike Barnes
Acting Assistant Special Agent in Charge
Secret Service
Why it Matters / What’s at Stake?

- Brand Risk / Client Experience
- Fraud Prevention
- Legal Risk
- Regulatory Risk
- Suspicious Activity Report Filing Requirements
- 2015 Regulatory Exam Priorities
  - SEC
  - FINRA
  - Cyber Security Breaches tied to BSA/AML Violations
- Fed/OCC/FDIC
  - OCC Comptroller Comments
- DOJ Concerns

Cyber security now crosses all security, compliance and business disciplines within an institution
– it is not just an information security or technology issue
Cybercrime – FinCEN SAR Definitions

Computer Intrusion
• For purposes of the FinCEN SAR, the term “computer intrusion” has been replaced by the term “unauthorized electronic intrusion”. The new term continues to be defined as gaining access to a computer system of a financial institution, to:
  • a. Remove, steal, procure, or otherwise affect funds of the institution or the institution’s customers;
  • b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information; and
  • c. Damage, disable or otherwise affect critical systems of the institution.

Account takeover
• “Account takeover” activity differs from other forms of computer intrusion, as the customer, rather than the financial institution maintaining the account, is the primary target.
• In an account takeover, at least one of the targets is a customer holding an account at the financial institution and the ultimate goal is to remove, steal, procure or otherwise affect funds of the targeted customer.
The Environment

• In 2015: the Internet Population was estimated at over 3 Billion Users (Over 42% of the World’s Population).
• US Survey: 60% Internet Users were on-line for at least 3 hours per day.
• Nearly 80% of all Smartphone users keep their phones with them, all but 2 hours of the waking day.
Cyber Threat Actors

- Nation State Actors
  - China
  - Russia
  - Iran
  - North Korea
- Criminal Actors & Organizations
- Hacktivists
- Insiders
  - Accidental
  - Intentional
Cyber Attacks

• Social engineering
  • email
  • social media
  • phone
  • in person
• Phishing
  • spear phishing
  • ID theft
  • email phishing
• Phone spoofing / Phone porting
• DDOS
• Remote Access Tools
Key Cyber Trends

- Financial Accounts Targeted Phishing Attacks
- Client Account Take-Overs
- Business Email Compromise
  - Executive Management Email Spoofing
- Romance Scams
- Title Company Wire Direction Hijacking
- Business Opportunities / Work at Home
- IRS False Filing / Imposter Scams
- Lottery Fraud
- Penny Stock Fraud
  - Account Take-Overs; Cyber Intrusions; Social Engineering
Financial Institutions Cyber Best Practices

BSA/AML

Law Enforcement

Security

Cyber Security / IT

Fraud
Key Membership Groups

- ACAMS
- Financial Services Information Sharing Analysis Center (FS-ISAC)
- National Cyber Forensic Training Alliance
- FBI InfraGard
- USSS Electronic Task Force
- FBI Cyber Task Force
Q&A from the Audience

Our Moderator:

Greg Ruppert
Vice President
Financial Crimes Investigations
Charles Schwab

Our Panelists:

Chris Wallace
Lead Intelligence Analyst
CenturyLink

Tim Wallach
Supervisory Special Agent
Federal Bureau of Investigation

Ike Barnes
Acting Assistant Special Agent in Charge
Secret Service