2016 Cyberspace Law Institute and Winter Working Meeting
American Bar Association

January 29 - 30, 2016

Kevin D. Rosen, Senior Regional Counsel, FINRA Enforcement

FINRA™
Financial Industry Regulatory Authority

1 Financial Industry Regulatory Authority

Financial Industry Regulatory Authority

- FINRA is dedicated to investor protection and market integrity through effective and efficient regulation of the securities industry
- FINRA is not part of the government
- FINRA is an independent, non-for-profit organization authorized by Congress to protect America's investors by making sure the securities industry operates fairly and honestly
- FINRA does this by:
  - Writing and enforcing rules that govern the activities of securities firms and brokers
  - Examining firms for compliance with those rules
  - Fostering market transparency
  - Educating investors

Financial Industry Regulatory Authority

FINRA BY THE NUMBERS

3,500 employees dedicated to market integrity and investor protection

17 offices across the U.S.

More than 700 fraud cases referred for prosecution in 2014

$166.3M in fines and restitution levied in 2014

30 billion on average—and **up to 50 billion**—transactions processed every day

642,981 brokers under FINRA's supervision

2 Cybercrime and Cybersecurity

Financial Industry Regulatory Authority

The Alert Investor

WHO ARE THE HACKERS?

The landscape of threat actors includes cybercriminals whose objective may be to steal money or information for commercial gain, nation-states that may acquire information to advance national objectives, and hacktivists whose objectives may be to disrupt and embarrass an entity.

The Alert Investor

FINRA "Report on Cybersecurity Practices," February 2015

The Alert Investor

Source: The Alert Investor (May 27, 2015)

The Alert Investor

FINRA "Investor Alerts: Cybersecurity and Your Brokerage Firm," February 3, 2015

The Alert Investor

3 FINRA Cybersecurity Report
February 2015

Financial Industry Regulatory Authority

Summary of FINRA Report

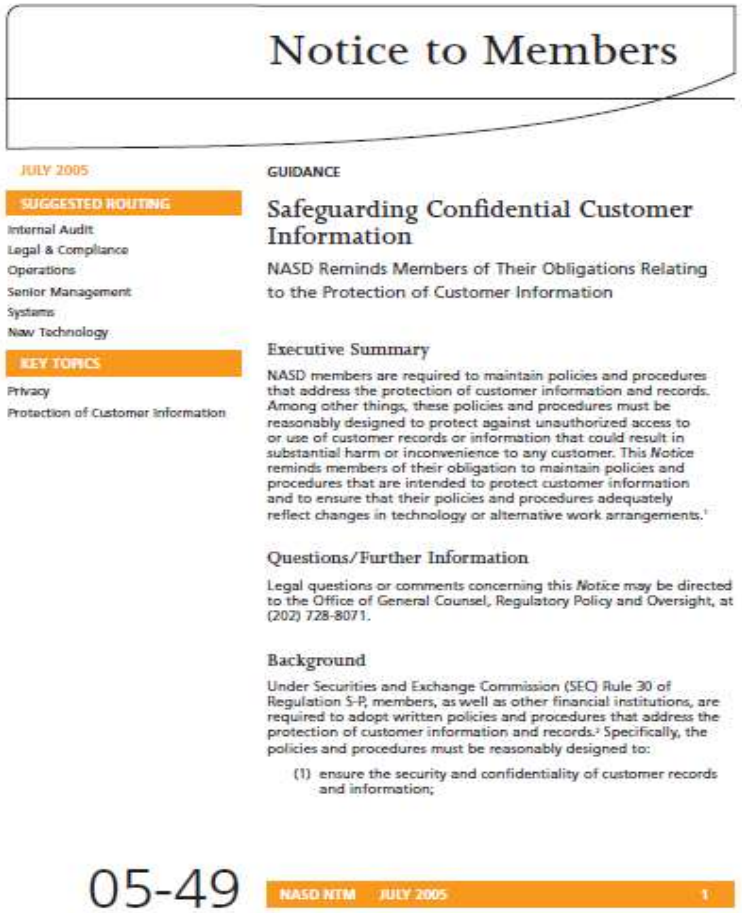
- Sound governance framework – strong leadership
- Risk assessments tools for firms to understand cybersecurity risks
- Technical controls are highly contingent on firms' individual situations
- Develop, implement and test incident response plans
- Exercise strong cybersecurity due diligence with vendors
- Well-trained staff is important defense against cyberattacks
- Intelligence-sharing opportunities to protect against cyber threats

4 Regulations and Rules

Potential Violations

- FINRA Rule 3110 – Supervision
- FINRA Rule 3310 – Anti-Money Laundering
- FINRA Rule 3130 – Annual Certification of Compliance and Supervisory Process
- FINRA Rule 4370 – Business Continuity Plans and Emergency Contact Information
- SEC Regulation S-P – Safeguard Customer Records and Information
- SEC Regulation S-ID – Identity Theft Red Flags
- SEC Rule 17a-4(f) – Preservation of Records

Notice to Members 05-49



Notice to Members

JULY 2005

SUGGESTED ROUTING

Internal Audit
Legal & Compliance
Operations
Senior Management
Systems
New Technology

KEY TOPICS

Privacy
Protection of Customer Information

GUIDANCE

Safeguarding Confidential Customer Information

NASD Reminds Members of Their Obligations Relating to the Protection of Customer Information

Executive Summary

NASD members are required to maintain policies and procedures that address the protection of customer information and records. Among other things, these policies and procedures must be reasonably designed to protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. This *Notice* reminds members of their obligation to maintain policies and procedures that are intended to protect customer information and to ensure that their policies and procedures adequately reflect changes in technology or alternative work arrangements.[1]

Questions/Further Information

Legal questions or comments concerning this *Notice* may be directed to the Office of General Counsel, Regulatory Policy and Oversight, at (202) 728-8071.

Background

Under Securities and Exchange Commission (SEC) Rule 30 of Regulation S-P, members, as well as other financial institutions, are required to adopt written policies and procedures that address the protection of customer information and records.[2] Specifically, the policies and procedures must be reasonably designed to:

(1) ensure the security and confidentiality of customer records and information;

05-49

NASD NTM JULY 2005 1

Regulatory Notice 12-05

Regulatory Notice 12-05

Customer Account Protection

Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts

Executive Summary

FINRA has received an increasing number of reports of incidents of customer funds stolen as a result of instructions emailed to firms from customer email accounts that have been compromised. These incidents highlight some of the risks associated with accepting instructions to transmit or withdraw funds via email. FINRA recommends that firms reassess their policies and procedures to ensure they are adequate to protect customer assets from such risks. The Federal Bureau of Investigation (FBI), Financial Services Information Sharing and Analysis Center (FS-ISAC) and Internet Crime Complaint Center (IC3) recently released a joint fraud alert describing a similar trend.[1]

Questions concerning this *Notice* should be addressed to:

- Patricia Albrecht, Associate General Counsel, Office of General Counsel, at (202) 728-8026; or
- Terry H. Miller, Lead Sr. Regulatory Specialist, Member Regulation Department, at (202) 728-8159.

Background and Discussion

FINRA has received an increasing number of reports of incidents in which firms have wired customer funds to third-party accounts based on instructions received from customers' email accounts that had been compromised by third parties. In some instances, the perpetrators appear to have obtained customers' brokerage information by accessing customers' email accounts and searching contact lists or emails sent from the account. Typically, the perpetrators of these fraudulent schemes email brokerage firms from customers' personal email accounts with instructions to wire funds to an account, often overseas, controlled by the perpetrator. The instructions may be accompanied or followed by fraudulent letters of authorization also emailed from compromised email accounts. In some instances, firms have released funds after unsuccessfully attempting to verify emailed instructions by phone. In at least one case, the fraudulent email stressed the urgency of the requested transfer, pressuring the firm to release the funds before verifying the authenticity of the emailed instructions.

FINRA Financial Industry Regulatory Authority

January 2012

Notice Type
- Special Alert

Suggested Routing
- Operations
- Senior Management
- Systems

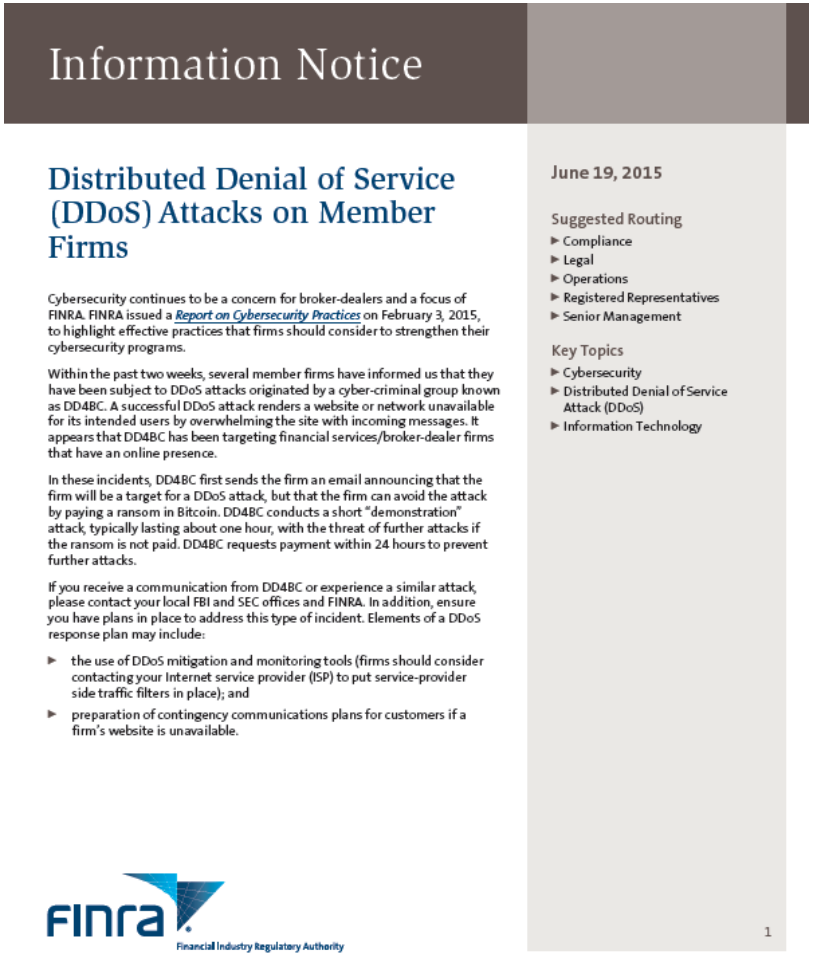
Key Topics
- Customer Account Protection

Referenced Rules & Notices
- FINRA Rule 4311
- FTC FACT Act
- NASD Rule 3012
- NYSE Rule 401
- Regulatory Notice 08-69
- Regulatory Notice 09-64

1

FINRA

Information Notice



Information Notice

Distributed Denial of Service (DDoS) Attacks on Member Firms

Cybersecurity continues to be a concern for broker-dealers and a focus of FINRA. FINRA issued a *Report on Cybersecurity Practices* on February 3, 2015, to highlight effective practices that firms should consider to strengthen their cybersecurity programs.

Within the past two weeks, several member firms have informed us that they have been subject to DDoS attacks originated by a cyber-criminal group known as DD4BC. A successful DDoS attack renders a website or network unavailable for its intended users by overwhelming the site with incoming messages. It appears that DD4BC has been targeting financial services/broker-dealer firms that have an online presence.

In these incidents, DD4BC first sends the firm an email announcing that the firm will be a target for a DDoS attack, but that the firm can avoid the attack by paying a ransom in Bitcoin. DD4BC conducts a short "demonstration" attack, typically lasting about one hour, with the threat of further attacks if the ransom is not paid. DD4BC requests payment within 24 hours to prevent further attacks.

If you receive a communication from DD4BC or experience a similar attack, please contact your local FBI and SEC offices and FINRA. In addition, ensure you have plans in place to address this type of incident. Elements of a DDoS response plan may include:

- the use of DDoS mitigation and monitoring tools (firms should consider contacting your Internet service provider (ISP) to put service-provider side traffic filters in place); and
- preparation of contingency communications plans for customers if a firm's website is unavailable.

FINRA
Financial Industry Regulatory Authority

June 19, 2015

Suggested Routing
- Compliance
- Legal
- Operations
- Registered Representatives
- Senior Management

Key Topics
- Cybersecurity
- Distributed Denial of Service Attack (DDoS)
- Information Technology

1

FINRA

5 Formal Disciplinary Action

FINRA™
Financial Industry Regulatory Authority

Case Study

SQL Injection and Exfiltration of Customer Information

- Firm failed to establish and maintain a supervisory system reasonably designed to safeguard confidential customer information
- Firm failed to adopt and implement policies and procedures reasonably designed to safeguard customer records and information
- Firm failed to protect certain confidential information of its customers when it utilized a database server containing customer account numbers, social security numbers, names, addresses, dates of birth, and certain other confidential data, but without adequate safeguards to protect the security and confidentiality of that information
- The Firm's failure permitted international criminals to improperly access, by a computer hack, the confidential customer information of approximately 192,000 customers

SQL Injection and Exfiltration of Customer Information

- The Firm employed a public facing computer web server that hosted certain Firm web pages behind an external perimeter firewall
- Same computer housed the database with the customer confidential information and had persistent internet connection
- Database never encrypted and password not activated
- December 26 - 27, 2007, the database was compromised by a third-party hacker who downloaded the confidential information through a sophisticated network intrusion (SQL injection)
- Perpetrator, believed to be part of international crime syndicate, demanded ransom for data

SQL Injection and Exfiltration of Customer Information

- The attack was visible on the Firm's web server logs, which were not reviewed by the Firm
- Firm had no procedures to review logs or to respond to network intrusion, even though Firm's independent auditor had recommended the implementation of an intrusion detection system, prior to the attack
- As a result, the Firm violated Regulation S-P of the Securities Exchange Act of 1934, and NASD Rules 3010 and 2110

SQL Injection and Exfiltration of Customer Information

- Firm remedial action:
  1. Took down website and reported matter to law enforcement
  2. Hired outside firm to enhance network security, encryption and detection
  3. Provided significant cooperation to law enforcement
  4. Issued press release, notified customers, offered credit monitoring to customers, and resolved class action litigation
- FINRA sanctions against the Firm:
  1. Censure
  2. $375,000 fine

Case Study

Lost Unencrypted Laptop with Confidential Customer Information

- Firm failed to establish and maintain a supervisory system reasonably designed to safeguard confidential customer information
- From March 2009 through June 2014, the Firm's written supervisory procedures were not reasonably designed to protect confidential customer and proprietary information.
- There were insufficient supervisory procedures to ensure that the Firm's "most sensitive" customer and proprietary information stored on laptops were being adequately safeguarded by appropriate technology

Lost Unencrypted Laptop with Confidential Customer Information

- March 2009 – Firm recognized the need for encryption of laptops, but considered it a “moderate risk” due to a low laptop count
- April 26, 2010 – Firm approved an Information Security Program Charter, but it did not require the encryption of laptops
- Year 2010 – Firm purchased Microsoft Enterprise Agreement software to encrypt laptops
- Year 2012 (approximately) – Management did not authorize additional funds to add personnel to implement new encryption software
- Year 2012 – Firm hired two additional security analysts to install encryption software, which was determined to be incompatible

Lost Unencrypted Laptop with Confidential Customer Information

- 2012 through 2nd Quarter 2013 – Employee turnover
- 3rd Quarter 2013 – Firm identified new encryption solution and proposed funding was requested to outsource intrusion detection and data-loss prevention services
- May 29, 2014 – Firm IT employee inadvertently left unencrypted laptop in a restroom and it was lost:
  - Personal and confidential information of 352,551 customers placed at risk
  - Believed to contain two highly sensitive files, including account numbers, customer names and addresses, and tax identification numbers, over a period of approximately 20 years
- June 2014 – Firm management approved funding, following the unencrypted laptop loss

Lost Unencrypted Laptop with Confidential Customer Information

- Firm's written supervisory procedures did not adequately address the technology in use, specifically laptops
- Firm failed to take appropriate technological precautions to protect customer and highly sensitive information
- Firm had no written supervisory procedures to ensure that the Firm's most sensitive customer and proprietary information stored on laptops were being adequately safeguarded by appropriate technology, such as encryption
- Firm's failure to adopt written supervisory procedures reasonably designed to insure the security of customer information placed sensitive customer information at risk
- As a result, the Firm violated Regulation S-P of the Securities Exchange Act of 1934 and FINRA Rule 2010

Lost Unencrypted Laptop with Confidential Customer Information

- FINRA sanctions against the Firm:
  1. Censure
  2. $225,000 fine
  3. Firm undertaking to conduct an internal review of the adequacy of its policies, systems and procedures (written and otherwise) and training relating to compliance with Regulation S-P
  4. Firm undertaking to correct violations identified in AWC
  5. Firm certification that it has in place adequate written supervisory procedures to comply with Regulation S-P

Case Study

Identify Thief – Account Intrusion

- For approximately 26 months, Firm did not adequately follow-up on red flags with regard to certain transfers from a particular customer's account that appeared on exception reports that the Firm used to identify potentially suspicious activity
- As a result, an identity thief, who hacked a customer's account, was able to cause unauthorized stock sales and misappropriate a total of $452,100 from the Firm's customer by way of six ACH electronic fund transfers to an outside bank account not in the customer's name

Identify Thief – Account Intrusion

- **Red flags that Firm failed to adequately respond:**

1. Customer's online account was repeatedly accessed from what appeared to be a Texas IP address (when the customer lived in Illinois)

2. E-mail address associated with the account was changed from a Texas IP address

3. There were multiple failed attempts to reset the account security PIN from a Texas IP address

4. Identity thief, pretending to be the firm customer, called the Firm's customer service center and was unable to verify security questions

Identify Thief – Account Intrusion

- **Red flags that Firm failed to adequately respond:**

5. Identity thief called from a Skype phone account and could not answer the security question (the customer's mother's maiden name)

6. Firm employee who took the call failed to escalate the matter to appropriate personnel at the Firm

7. Firm failed to adequately review its Large ACH Report which raised numerous "red flags"

Identify Thief – Account Intrusion

- By failing to implement written policies and procedures reasonably designed to review and monitor ACH transfers of funds from customer accounts to outside bank accounts, the Firm violated NASD Rule 3012 and FINRA Rule 2010
- By failing to adequately respond to red flags relating to transmittals of a particular customer's funds, the Firm violated NASD Rule 3010 and FINRA Rule 2010
- FINRA sanctions against the Firm:
  1. Censure
  2. $150,000 fine

Case Study

Customer Impersonation, E-mail Hack and Wire Fraud

- In January 2015, a registered representative (RR) submitted for processing two fraudulent wire transfer requests totaling $70,500 from the account of a Firm customer to third-party bank accounts
- RR submitted the wire transfers for processing based on e-mail instructions that she received from an imposter posing as the Firm customer who had hacked into the customer's e-mail account
- In connection with the wire transfer requests, RR had falsely completed and submitted two wire request forms, stating on each form that she had verbally confirmed each wire transfer request with the customer which she had not done

Customer Impersonation, E-mail Hack and Wire Fraud

- The Firm effected the first wire in the amount of $20,500
- The Firm's Cashiering Department rejected the second wire in the amount of $50,000 because the customer's signature was identical on both wire request forms
- The Firm's Cashiering Department insisted that RR call the customer to confirm the wire requests
- RR called the customer and learned that the wire requests were fraudulent
- The Firm was unable to recover the first wire and reimbursed the customer $20,500

Customer Impersonation, E-mail Hack and Wire Fraud

- By falsifying the Firm's records and making false statements to the Firm's personnel regarding receiving verbal confirmation from the Firm's customer, RR violated FINRA Rule 2010
- The false attestations that RR made on the wire request forms caused the Firm's books and records to be inaccurate, in contravention of the Firm's obligation to maintain accurate books and records - therefore, RR violated FINRA Rules 4511 and 2010
- FINRA sanctions against RR, who had no relevant disciplinary history:
  1. 30 calendar day suspension from association with any FINRA member in any capacity
  2. $5,000 fine