# Data Privacy And Cybersecurity For Investment Funds

Gregory J. Nowak | Angelo A. Stio III | October 28, 2014

Pepper Hamilton LLP
Attorneys at Law

# WHY IS DATA PRIVACY AND SECURITY IMPORTANT?

# Why is it important to protect data?

- Data privacy is not just for big tech; it impacts all organizations that collect sensitive data
  - Networks
  - Copiers
  - Smart phones
  - Laptops
  - Credit card processing
- Significant risks of non-compliance
  - Harm to individual
  - Costs of notice and remediation
  - Regulatory actions/Fines and penalties
  - Potential lawsuits
  - Loss of business, resources and employee time
  - Damage to brand and reputation
  - Disruption

# Why is it important to protect data?

- "This is a global threat. Cyber threats are of extraordinary and long-term seriousness. They are first on the Division of Intelligence's list of global threats, even surpassing terrorism. And Jim Comey, director of the FBI, has testified that resources devoted to cyber-based threats are expected `to eclipse' resources devoted to terrorism." **Chair Mary Jo White - SEC Cybersecurity Roundtable – March 26, 2014**
- FINRA is especially concerned about smaller firms, as exams have shown particular vulnerability in technology systems, with problems that include expired or ineffective anti-viral software. **Susan Axelrod and Michael Rufino at the February 25, 2013, meeting of the SRO Subcommittee of the ABA Securities Litigation Committee**

# SEC Cybersecurity Risk Alert

- The SEC's Office of Compliance Inspections and Examinations (OCIE) issued a risk alert on its cybersecurity initiative on April 15, 2014.
- The OCIE will initially examine 50+ broker-dealers and registered investment advisers re cybersecurity issues, with a focus on the following issues:
  - Cybersecurity governance; identification & assessment of cybersecurity risks; protection of networks & information; remote customer access and funds transfers; vendors & third parties; detection of unauthorized activity; and experiences with certain cybersecurity threats.

# FINRA Scrutiny

- January 2, 2014 Annual Regulatory and Examination Priorities Letter:
  - Identified “Cybersecurity” as a priority.
  - Expressed concern about the integrity of firms’ infrastructure and the safety and security of sensitive customer data.
  - Primary focus is integrity of firms’ **policies**, **procedures** and **controls** to protect sensitive customer data.
  - Evaluation of such controls may take the form of examinations and targeted investigations.

# FINRA Scrutiny

- February 6, 2014 Launch of Cybersecurity Sweep
  - Assessment, via targeted letters, of broker-dealers' approaches to managing cybersecurity threats and protecting their IT structure.
  - Four stated goals:
    - 1. To understand better the types of threats that firms face;
    - 2. To increase FINRA's understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their IT system;
    - 3. To understand better firms' approaches to managing these threats, including through risk assessment processes, IT protocols, application management practices and supervisions; and
    - 4. As appropriate, to share FINRA's observations and findings with firms.
  - Survey can be found at: http://www.finra.org/web/groups/industry/documents/industry/p443220.pdf.

# FINRA Scrutiny

- February 6, 2014 Launch of Cybersecurity Sweep (cont.)
- Assessment to focus on the following:
  - Approaches to IT risk assessment;
  - Business continuity plans in case of cyber-attack;
  - Organization structures and reporting lines;
  - Processes for sharing and obtaining information about cybersecurity threats;
  - Understanding of concerns and threats faced by the industry
  - Assessment of the impact of cyber-attacks on the firm over the past 12 months;
  - Approaches to handling denial of service attacks;
  - Training programs;
  - Insurance coverage for cybersecurity-related events; and
  - Contractual arrangements with third-party services providers.

# BEFORE THE BREACH

# What is the definition of a security breach?

- **Security Breach Definition** -
  - Unauthorized access to electronic files, media or data containing Personal Information
  - Access compromises the security, confidentiality or integrity of the Personal Information (“PI”)
  - Where the PI has not otherwise been secured by encryption or by any other method or technology that renders the PI unreadable or unusable.

# What is Personally Identifiable Information?

- **Personally Identifiable Information (PII)** is any information relating to an identified or identifiable natural person.
- PII includes any piece of information which can be used to uniquely identify or trace an individual's identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual.
- Data elements vary by state/statute
- Combination/factor analysis

Pepper Hamilton LLP
Attorneys at Law

# What is Personally Identifiable Information?

## Typical PII data elements include:

- Full name
- National identification number/ Social Security Number (SSN) in U.S.
- Date of birth
- Driver's license number
- Passport number
- Biometric records face, finger prints, handwriting samples, voice prints, other biometric identifiers
- Credit card and financial account numbers
- Telephone number
- Street address
- Zip code
- Email address
- Voice recordings
- Digital identifiers
- "Sensitive" information demographic information, gender, citizenship, racial or ethnic origin, medical or health information (including accommodations), religious beliefs or affiliation, political opinions

# Biggest cyber-security threats

## Top Threats to Data Privacy

1. Your personnel
   - Negligence (or maliciousness)
     - Loss or theft of laptop & mobile devises are the foremost case of data breaches
   - Unintended disclosure due to negligence and clerical errors
     - Email distribution list vs. individuals
     - Non-encrypted communication
     - Policy violations
   - Loss of a portable data storage device
     - USB-Flash-Drives
     - Unauthorized Cloud Storage
     - Lost or missing back up tapes

Pepper Hamilton LLP
Attorneys at Law

# Biggest Cyber-security Threats

## Top Threats to Data Privacy

2. Advanced Persistent Threat (APT)
   - Foreign Governments, Political Activists and Organized Crime
     - Capability and intent to persistently and effectively target a specific entity
       - Biggest PII targets include higher education and financial institutions
       - Also targeting defense, energy and pharmaceutical companies
       - Focus is on systems, current and former employees including retirees, independent contractors, consultants

# Before a Breach

## Address Breach Before It Occurs

- Annual Risk Assessments
  - Identify where PII is located
  - Analyze flow of PII
  - Who has access
  - How is PII collected, transmitted, stored, discarded
- Comprehensive Security Program
  - Implement controls
  - Third parties
- Safeguard Categories
  - Physical
  - Administrative
  - Technical

- Privacy and Security Policy
- Risk Mitigation
  - Corporate Rules
  - Insurance
  - Training and Education

# Regulation S-P (17 C.F.R. § 248)

- **Privacy Rule**
  - Privacy rule for financial institutions, including brokers, dealers, investment companies, and investment advisors.
  - Nonpublic Personal Information: personally identifiable financial information, including lists based on such information
  - Purpose:
    - Requires notice to customers about privacy practices and policies;
    - Describes conditions under which a financial institution may disclose nonpublic personal information;
    - Provides opt-out mechanism for consumers

# Regulation S-P (17 C.F.R. § 248)

- Must provide a clear and conspicuous notice that accurately reflects privacy policies and practices. 17 C.F.R. § 248.4
- Must provide notices initially, annually, and as revised. 17 C.F.R. §§ 248.4, 248.5, 248.8
- Notices must identify the categories of information collected and disclosed and the entities to whom the information is disclosed; also must include an explanation of the opt out right and methods, FCRA disclosures, and policies and practices for protecting information. 17 C.F.R. § 248.6

# Regulation S-P (17 C.F.R. § 248)

- Form and method of opt out notice must comply with 17 C.F.R. § 248.7.
- Must deliver privacy and opt out notices “so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.” 17 C.F.R. § 248.9
- Must not disclosure nonpublic personal information unless privacy and opt out notices are given and consumer does not opt out after a reasonable opportunity to do so. 17 C.F.R. § 248.10

# Regulation S-P (17 C.F.R. § 248)

- Must not disclose consumer's account number or access code for credit, deposit, or transaction account to a nonaffiliated third party, subject to limited exceptions. 17 C.F.R. § 248.12
- Exceptions to privacy and opt out notices exist for joint marketing agreements, transactions authorized by the consumer, and other specific instances. 17 C.F.R. §§ 248.13, 248.14, 248.15

# Regulation S-P

- **Rule 30 – Safeguard Procedures**:
  - adopt written policies and procedures for the protection of customer information and records
    - Administrative
    - Technical
    - Physical
  - protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information .

*17 CFR 248.30*

- **State Privacy Laws**
  - 47 States have data breach notification legislation
    - States without: Al, NM, SD
  - States also have legislation governing security of personal information
    - Many states broader protections than federal (CA, MA, NV)
  - Federal privacy legislation generally does not control/preempt state laws.

## Notification Obligation - Majority Rule

- **Two-prong analysis**
  - Disclose any breach of security following discovery if reasonable basis to believe (1) personal Information has been accessed by an unauthorized person, and (2) is subject to being misused
  - Some states only have single-prong approach (CT, NJ, PR)

# Notification Obligation - Majority Rule

- **Who to notify?**
  - Customer (most expedient time possible and without unreasonable delay)
  - Consumer reporting agencies (if more than 1,000 customers impacted)
  - Law enforcement (before notifying customers)

# Notification Obligation - Majority Rule

- **Others to notify**
  - Insurance carrier
  - Regulators
  - If maintaining/collecting PII for another entity, you must notify that entity

# Addressing a Breach

- You should also consider whether the following must/should be notified:
  - Insurance carrier
  - Regulators
  - If maintaining/collecting PI for another entity, you must notify that entity
  - Contract parties about potential indemnification

# ADDRESSING A BREACH

# Addressing a Breach

## Have Preparedness Plan and Response Team in Place

- The first 24 hrs
  - Record date/time
  - Activate team
  - Secure area/evidence
  - STOP FURTHER DATA LOSS
  - Identify internal personnel to take statements
  - Follow plan
  - Contact forensic firm and law enforcement
  - Executive communications and notification team

"Careful! He knows computers."

# Addressing a Breach

## Document Information Related to Breach

- Date of breach
- How discovered
- Person who made discovery
- Description of incident and root cause
- Date and how system was secured
- # of individuals affected
- Type of information accessed
- Did it result in acquisition of PI
- Is there possibility of misuse
- Steps to mitigate damages/control breach
- Steps you've taken to prevent future occurrence
- Notice – When and How
- Residence of individuals affected
- Services offered to customers to lessen potential harm
- Public relations message

# Addressing a Breach

- FINRA Checklist for Compromised Accounts
  - Monitor, limit or temporarily suspend activity in the account
  - Alert others in firm
  - Identify, if possible, root cause
  - If firm is not self-clearing, notify clearing firm
  - Contact SEC and FINRA Coordinator
  - Contact law enforcement agencies
  - Contact relevant state regulatory authorities
  - Contact customer and, if appropriate, change password and/or account number
  - Comply with state data breach notification laws
  - Determine whether firm must file a suspicious activity report (SAR) under federal anti-money laundering provisions
  - Copy of checklist can be found at: http://www.finra.org/Industry/Issues/CustomerInformationProtection/P117443

# AFTER A BREACH

# After a Breach

- **Litigation**
  - Direct actions
  - Class Actions
    - Consumer
    - Shareholder
    - Banks/Credit Unions
  - Derivative Suits
    - Director and Officer Liability

# Litigation

- *In re Choicepoint*, No. 1:05-CV-00686-JTC, 2006 U.S. Dist. LEXIS 97903 (N.D. Ga. Nov. 19, 2006)
  - Shareholder class action; alleged defendants concealed and misrepresented the existence and severity of data and privacy security problems.
  - Company marketed its data security measures "as beyond those mandated by law;" data breaches disclosed; shares fell 17% in three weeks.
  - Court denied motion to dismiss claims for damages under Sections 10(b) and 20(a) related to false and misleading statements.

# FINRA – Regulatory Action

- SEC and FINRA have brought more than 10 enforcement actions related to data privacy and security:
  - **1. Cybersecurity governance**
    - Failure to enforce written cybersecurity procedures.
    - Failure to perform periodic assessments or inadequate periodic inspections.
  - **2. Protection of firm networks and customer information**
    - Failing to encrypt nonpublic customer information.
    - Inadequate antivirus software/firewalls.
  - **3. Vendors and outsourcing**
    - Failing to ensure third-parties follow cybersecurity policies.
  - **4. Responding to cybersecurity braches**
    - Inadequate customer and regulatory authority notifications.

# FINRA – Regulatory Action

- FINRA fined broker-dealer and financial advisor $600,000, saying the units had no idea who was accessing client records for years at a time.
- FINRA fined firm $375,000 for failure to protect confidential customer information.
  - Failure to have adequate security to protect hacking.
  - Failure to monitor logs that would have uncovered hacking.
- FINRA fined firm $150,000 because customer had unauthorized online viewing access to unrelated customer accounts for approximately six months and firm did not notify affected customers for more than a year.
- FINRA fined and suspended broker for downloading confidential customer information from his firm's computer system on his last day of employment and then sharing that information with new firm.

# OCIE CYBERSECURITY INITIATIVE

# SEC Cybersecurity Risk Alert – Sample Requests

- Issue:  Identification of Risks/Cybersecurity Governance
  - Details re inventorying and monitoring hardware, software, network, and programs;
  - Written information security policy;
  - Details of periodic cybersecurity risk assessments;
  - Details of physical security risk assessments related to cybersecurity;
  - Written documentation re role of workforce responsible for cybersecurity;
  - Written business continuity plan re cybersecurity incident and/or recovery;
  - Identity of Chief Information Security Officer;
  - Details re insurance coverage for cybersecurity incidents

# SEC Cybersecurity Risk Alert – Sample Requests

- Issue: Protection of Firm Networks & Information
  - Identify cybersecurity risk management process standards (e.g., NIST, ISO) used to model firm's information security;
  - Provide existing policies and procedures re 12+ initiatives related to user access, asset management, data destruction, encryption, and compliance auditing

# SEC Cybersecurity Risk Alert – Sample Requests

- Issue: Risks Associated with Remote Customer Access & Funds Transfer Requests
  - Details re management, functionality, and security of on-line account access;
  - Procedures for verifying authenticity e-mail requests to transfer customer funds;
  - Policies for addressing responsibility for losses associated with attacks or intrusions that impact customers

# SEC Cybersecurity Risk Alert – Sample Requests

- Issue: Risks Associated with Vendors & Other Third Parties
  - Details of cybersecurity risk assessments conducted of vendors and business partners;
  - Details of cybersecurity requirement incorporated into contracts with vendors and business partners;
  - Details of segregating sensitive network resources from third parties;
  - Details of controls, policies, and procedures in place to control network access by vendors, business partners, or other third parties

# SEC Cybersecurity Risk Alert – Sample Requests

- Topic:  Detection of Unauthorized Activity
  - Details of practices and procedures for activities related to detecting, reporting, and preventing suspected unauthorized activity

# SEC Cybersecurity Risk Alert – Sample Requests

- Other Areas
  - Incorporation of the 2013 Identity Theft Red Flag Rules (17 C.F.R. § 248 – Subpart C – Regulation S-ID);
  - Methods for determining cybersecurity best practices;
  - Summaries of the following events since 1/1/13:
    - Malware detected on firm device;
    - Firm website or network blocked because of online attack;
    - Website or network impairment caused by software malfunction;
    - Network breached by unauthorized user;
    - Compromise of a customer's or vendor's computer allowed fraudulent activity to be conducted on network;
    - Firm received fraudulent e-mails purportedly from customers
    - Extortion attempts based on threats of network damage;
    - Misconduct by authorized network users resulting in misappropriation of funds or information

# SEC Cybersecurity Risk Alert – Sample Requests

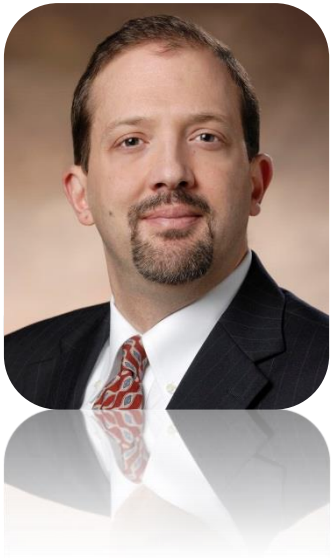
- Other Areas (cont'd)
  - Details of theft, unauthorized exposure, or similar event related to customer information, since 1/1/13;
  - Reporting of fraudulent or unauthorized activity to law enforcement, FinCen, FINRA, state/federal agency, industry or public-private organization;
  - Details of the three most serious cybersecurity risks;
  - Any other information helpful for evaluating the firm's cybersecurity posture

# Gregory J. Nowak

215.981.4893
nowakg@pepperlaw.com

- Partner in the Financial Services Practice Group
- Concentrates his practice in securities law, particularly in representing investment management companies and other clients on matters arising under the Investment Company Act of 1940 and the related Investment Advisers Act of 1940, and broker dealers and commodity futures traders and pool operators
- Represents many hedge funds and other alternative investment funds in fund formation, investment and compliance matters, including compliance audits and preparation work
- Writes and speaks frequently on issues involving investment management, health care and other matters and is the author of four books on hedge funds.

# Angelo A. Stio III



609.951.4125
stioa@pepperlaw.com

- Partner in the Litigation and Dispute Resolution Department of Pepper Hamilton LLP, and a member of the firm's Privacy, Security and Data Protection group where he regularly counsels health care, financial services and educational institution clients on data privacy and security issues
- An experienced trial attorney who litigates matters in state and federal courts throughout the country. He has been included in the annual *New Jersey Super Lawyers* lists for 2011-2014 for business litigation. He handles complex commercial disputes, class actions and derivative suits, corporate governance disputes, and college and university litigations.




Pepper Hamilton LLP
Attorneys at Law