

Documents and Information Frequently Requested by the SEC During Privacy and Safeguarding Exams

I. Information Security Policies

- A. Written policies and procedures addressing administrative, technical, and physical safeguarding of customer records and information
- Enterprise-wide/high-level (including information relating to board or senior-management approval)
- B. All second- and third-tier policies/guidelines addressing Information Security policies and procedures (detailed policies and procedures down to the employee level) that include procedures for:
- Electronic data movement and storage
 - Paper records
 - Levels of employee use or access to data, and other policies relating to employee obligation for information security

II. Information Security Management Structure

- A. Governing bodies and committees overseeing or having input in the development, implementation, and maintenance of the firm's information security program
- Committee charters, minutes, reports, and other documentation evidencing oversight activities
 - Documentation showing interaction with key executives and levels of authority to take action
 - Involvement of the board and senior management in reviewing and approving policies and otherwise being aware of threats, issues, noncompliance, etc.
- B. Chief Information/Security Officer
- Education/experience
 - Scope of responsibilities
 - Activities and accomplishments
 - Reporting authority
 - Reports to governing bodies

C. Information Security Department

- Responsibilities (policy development, monitoring, and enforcement)
- Staffing (including future plans)
- Education/training
- Projects and planning
- Budget (including future budget for staff and projects)
- Penetration testing and vulnerability management
- Intrusion detection systems
- Firewall configuration
- Patch management, upgrades, and workarounds
- Implementation of security advisories on vulnerabilities in software and hardware
- Server hardening
- Access control management
- Incident evaluation and response
- Physical security
- Encryption policies
- Employee access
- BCP plans
- Disposal policies

D. Audit/examination reports; third-party reviews (the SEC is very interested in how you formed your policies and whether you utilized a third-party to review your practices to determine if your practices conform with industry best practices)

- Security of customer activity online
- ID theft/ACH/fraud
- Account takeover

III. Outsourcing and Third-Party Access to Customer Information

A. General policies and procedures on outsourcing and the disclosure of nonpublic information to third parties

- Compliance policies for dealing with third parties – when is it allowed and under what circumstances?
- Written supervisory procedures (monitoring and review)
- Audit/board reports

B. Policies and procedures for selecting and monitoring service providers and disclosures to third parties

- Technology interfaces with service providers (encryption, etc.) – do you have a company-wide policy and how is it enforced?
 - Criteria for selecting service providers (due-diligence review)
 - Recordkeeping, safeguarding (including destruction policies), and storage obligations under Rule 17a-4
 - Contractual requirements; ensuring service providers are meeting those obligations
 - Inspection/auditing of service providers
 - Training of employees regarding company policy on dealing with service providers – do you build it into the contract/procurement policy?
- C. Policies and procedures for service providers with access to nonpublic information
- Maintaining contracts and monitoring performance
 - Clearly identifying the information the service providers process or create
 - Medium of storage/transfer; location; back-up; 17a-3 and 17a-4 compliant
 - Procedures for shipment and transfer of records between company locations and third-party locations
- D. Disclosure policies in the event of unauthorized access or disclosure of nonpublic information
- Crisis management team
 - Processes for contacting law enforcement, regulators, and clients

IV. Customer Identification Procedures

- A. Verification procedures for each method used by clients to access their accounts (Web, IVR, e-mail, mail, phone broker, in-person, etc.)
- Specific information requested from a person requesting access to customer records or information to verify his or her identity and authorization (e.g., social security number, account number, date of birth, address, last transaction information, password, pin number, mother's maiden name, signature guarantee, executed power of attorney, or secret question and answer)
 - Process for determining if information used to verify identity and authorization appear in documents mailed or e-mailed to the customer (e.g., confirmations, account statements, or proxies) when developing verification procedures (mail-theft concerns)
 - Steps taken, if any, to further verify a person's identity and authorization when the person seeks to change account

information (address) or engage in transactions, including changes of bank accounts, ACH or wire instructions, and the movement of the money

- Escalation procedures to further verify a person's identity and authorization when the nature of the contact is indicative of any red flag concerning identity and authorization
- Description of post-contact procedures followed, if any, to provide additional assurance of the authenticity of the person's identity and authorization (e.g., written confirmation mailed to the customer following completion of the contact)
- Returned mail/bounce-back procedures

B. Training – Programs for training employees regarding identity theft

- Scope of training and frequency administered (new and existing associates)
- Method by which it is determined which associates receive training
- Process for tracking training

C. New Accounts – New account procedures concerning customer identification at the time a new account is opened

- Closely tied to AML procedures – do you allow accounts to open when red flags are present?
- Returned mail/bounce-back procedures
- Wire transactions/funding when bank account information is different from brokerage account – what are your policies for money transfer?

D. Investigation – Procedures for investigating an attempt (successful or unsuccessful) to gain unauthorized access to customer records or information, and/or move customer assets out of the account, including organization charts and procedures relating to identity theft investigation for each of the departments and offices discussed during initial SEC meetings

V. Online Activity

A. Procedures for doing business online

- Agreements, form disclosures
- Opening/registration of accounts
- Logon/authentication
- Wire/ACH instructions/processing and transfer
- Changes in account information
- Security procedures (timeout)

- IP tracking, intrusion detection
- B. Education of clients
- C. Information as to what is being done to protect clients with “dirty” machines and accounts that have been compromised

VI. Privacy Policies and Procedures

- A. Privacy policies regarding use/sharing of nonpublic information
 - Types of information collected
 - Policies regarding use, sharing, and disclosure
 - Opt-out policies and how they are maintained
 - Change-of-status policies and how they are handled
 - Policies modified due to new third-party relationships
 - Privacy policy delivery and opt-out procedures
 - Who has access and why?
- B. Policies and procedures regarding the sharing of nonpublic information with third parties
 - Disclosures to service providers and unaffiliated third parties
 - Processes for monitoring/auditing of company information disclosure and sharing practices
 - Processes for monitoring contractual obligations