Privacy Policies and Procedures (Regulation S-P) 9.00

Introduction

Regulation S-P details certain privacy rules promulgated under *Section 504 of the Gramm-Leach Bliley Act*, which requires the SEC, and other federal agencies to adopt rules implementing notification requirements and restrictions on a financial institution's ability to disclose personal nonpublic information about its consumers and/or customers. All such policies and procedures pertaining to *Regulation S-P* shall be effective July 1, 2001, and shall remain in effect hereinafter unless otherwise revised.

9.01 Types of Privacy Notifications

Initial Notification

The Firm must provide a clear and conspicuous privacy notice that accurately reflects the Firm's policies and practices regarding the use and disclosure of personal nonpublic information to their clients. All initial notices must be issued to both "customers" and "consumers" of the Firm as defined by the Rule (*see Section 9.04 Initial Privacy Policy Notifications for definitions*).

Short-form Notification

The Firm may satisfy certain initial notification requirements by providing consumers with a short-form initial notice at the same time as the Firm delivers an opt out notice. In this case, the Firm must provide clear and conspicuous verbiage; must state Firm's policy; and must provide reasonable means for obtaining privacy notice.

Annual Notification

The Firm is required to provide a clear and conspicuous notice to all customers that accurately reflect the Firm's privacy policies and practices on an annual basis during the continuation of the customer relationship. The Firm must issue its privacy policy at least once in any 12 consecutive month period during the continuation of the customer relationship

Revised Notification

The Firm must provide a *revised* privacy notice that accurately reflects the Firm's policies and practices regarding the use and disclosure of personal nonpublic information to their clients. These notices are to be used when disclosing any new categories of information to any nonaffiliated third party, any personal nonpublic information to a new nonaffiliated third party, and any personal nonpublic information about a former customer.

9.02 Required Information on Privacy Notices

At a minimum, the Firm is required to include the following information and disclosures within their Privacy Notices or Privacy Policy Statements for distribution to customers:

Collection of Customer Information

The categories of non-public personal information that the Firm may *collect* such as:

- General customer information;
- Customer transaction information involving the Firm or its affiliates;
- Customer transaction information involving nonaffiliated third parties;
- Consumer-reporting agency information.

Disclosure of Customer Information

The categories of non-public personal information that the Firm may *disclose* such as:

- Categories of personal nonpublic information that you reserve the right to disclose in the future, but do not currently disclose as a few examples to illustrate the types of information in each category; and
- If the Firm reserves the right to disclose ALL of the personal nonpublic information about customers that the Firm collects, then a simple statement shall be sufficient without the use of such examples or categories.

Disclosure to Affiliated/Non-Affiliated Parties

An “affiliation” exists when one company "controls," is controlled by, or is under common control with another company. The definition includes both financial institutions and entities that are not financial institutions. The proposed rule also provides that a broker-dealer, fund, or registered adviser would be considered an affiliate of another company if the other company is regulated under Title V by one of the Agencies, and under that Agency's rules, the other entity would be affiliated with the broker-dealer, fund, or registered adviser.

Therefore, the categories of affiliates and nonaffiliated 3rd parties to whom the Firm may disclose nonpublic personal information, other than those to whom information is disclosed under an exception in *Section 502(e)* of the G-L-B Act such as the following information:

- Financial service providers;
- Non-financial companies;
- Other firms.

Former Customers

The Firm’s policies with respect to sharing information about former customers;

Third-Party Service Providers

The categories of information that are disclosed under agreements with 3rd party service providers and joint marketers and the categories of third parties providing the services such as the following:

- List the categories of personal nonpublic information the Firm will disclose; and
- State whether the third party is a service provider that performs marketing services on the Firm’s behalf or whether it is a financial institution with which the Firm has a joint marketing agreement.

Opt-Out Clause

A consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties;

Disclosure of Information Sharing with Affiliated Companies

Any disclosures regarding affiliate information sharing opt-outs a financial institution is providing under the Fair Credit Reporting Act; and

Security and Protection of Customer Information

The institution's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information such as the following information:

- Describe in general terms who is authorized to have access to the information; and
- State whether or not the Firm has security practices and procedures in place to ensure the confidentiality of information in accordance with the Firm's policies.

NOTE: Except as permitted by law, the Firm does not disclose any non-public personal information about current or former customer to any non-affiliated third parties (see Privacy Notice for additional information).

9.03 Initial Privacy Policy Notifications

The Firm must provide a clear and conspicuous privacy notice that accurately reflects the Firm's policies and practices regarding the use and disclosure of personal nonpublic information to the following clients:

Customers

Under the Rule, a "customer" is defined as any consumer who has a "customer relationship" with a financial institution. As such, customers should be issued initial privacy notices *no later than* the establishment of a customer relationship with the customer.

Consumers

Under the Rule, a "consumer" is defined as any individual (or his or her legal representative) who obtains, from a financial institution, financial products, or services that are to be used primarily for personal, family, or household purposes. Because "financial product or service" includes a financial institution's evaluation of an application or request to obtain a financial product or service, a person becomes a consumer even if the application or request is denied or withdrawn. As such, consumers should be issued initial privacy notices *before* the disclosure any personal nonpublic information about the consumer to any nonaffiliated 3rd parties.

When Initial Privacy Notice is *Not* Required

Any broker/dealer, investment company or investment adviser firm registered with the SEC under the Investment Advisers Act of 1940, is *not required* to provide an initial privacy notice under the following conditions:

- In the event that the Firm does not disclose any personal non-public information about the consumer to any nonaffiliated 3rd party; and

- The Firm does not have a customer relationship with a consumer as in the case of effecting a transaction, opening an account (introducing broker/dealer or otherwise), or enters into an advisory contract.

Exceptions to Allow Subsequent Delivery of Notice

The SEC has allowed for the issuance of the notice to occur within a "reasonable time" after the establishment of a customer relationship under the following circumstances:

- In the event that the establishment of a customer relationship is *not* at the customer's election (as in the case of a transferred account by a trustee selected by SIPC and appointed by the United States Court);

- If providing the notice would substantially delay the customer's transaction and the customer agrees to receive such notice at a later time period (as in the case where the customer agrees to enter into a customer relationship involving the prompt delivery of a financial product or services); and

- A nonaffiliated broker/dealer or investment adviser establishes a customer relationship between the Firm and customer without the Firm's knowledge. ►►

Implementation Strategy

Registered representatives are responsible for distributing the initial privacy notice upon establishing a new account. The Firm's designated principal shall review and approve the form and content of initial and annual privacy notices to be issued to each new customer account, and each year thereafter. All review of initial and annual notices should be properly documented and filed as evidence of approval.

9.04 Annual Privacy Policy Notifications

The Firm is required to provide a clear and conspicuous notice to all customers that accurately reflect the Firm's privacy policies and practices on an annual basis or at least once in any twelve (12) consecutive month period during the continuation of the customer relationship.

When Annual Privacy Notice is *Not* Required

The Firm is NOT REQUIRED to provide an annual privacy notice under the following conditions:

- A closed customer account;

- The termination of a customer's investment advisory contract;

- A customer is no longer the owner of record for securities the Firm has issued (for investment companies registered under the Investment Company Act of 1940); and

- If an Investment Company's customer is determined to be a lost security holder as defined in *17CFR240.17a-24(b).* ►►

Implementation Strategy

The Firm will send the annual privacy notice/opt-out clause to all clearing firm customers. Each registered representative is responsible for distributing the privacy notice/opt-out clause to their non-clearing firm customers on an annual basis. Registered representatives must confirm annually that they have sent the notice by signing a confirmation of delivery form. All confirmations will be maintained by the Firm. On an as needed basis, the Firm's designated principal shall review and approve the form and content of annual privacy policy notices as well as opt-out clauses and notifications. Each review shall be conducted to ensure that all relevant and up-to-date information is included. Additionally, each review of the annual privacy policy notices and opt-out clauses will be properly documented and recorded by initialing and dating each revised and/or amended form as evidence of review.

9.05 Revised Privacy Policy Notifications

The Firm's privacy policy notice must be revised and issued to its customers based on the following terms and conditions:

- Disclosure of any new category of personal nonpublic information about a customer to any nonaffiliated 3rd party;
- Disclosure of any personal nonpublic information to a new nonaffiliated third party; and
- Disclosure of any nonpublic personal information about a former customer to a nonaffiliated third party if that person has chosen to opt out of such disclosure. ►►

Implementation Strategy

The Firm's designated principal will review and approve any amendments and/or revisions to the Firm's privacy policy to ensure that it complies with the aforementioned requirements. All current and future amendments to the Firm's policy will be maintained at the main office and properly evidenced as an indication of review.

9.06 Delivery of Privacy Policy Notifications

The Firm shall deliver its privacy policy notices to each consumer in writing or in electronic form (if requested by the consumer). Customers will have "received" such a privacy policy notice if one or more of the following delivery methods occur:

- Hand-delivery of a printed notice copy to the consumer;
- Mail delivery of a notice copy to the last known address of the consumer;
- Electronic posting of a notice requiring the consumer to acknowledge receipt as a necessary step in obtaining a financial product or service;
- Electronic posting of a notice requiring the consumer to acknowledge receipt as a necessary step in obtaining a financial product or service.

9.07 Delivery of Opt-Out Notifications

If the Firm is required to provide an opt-out notice in accordance with the Rule, the Firm will provide a clear and conspicuous notice to the Firm' consumers that accurately explains their right to opt-out from disclosing personal nonpublic information to nonaffiliated third parties.

The opt-out notice must state the following information:

- The Firm's right to disclose nonpublic personal information about consumers to a nonaffiliated 3rd parties;
- The consumer's right to opt out of such disclosures;
- A reasonable means by which the consumer can exercise their right to opt out;
- A telephone number for consumers to call and opt out.

The Firm shall allow a reasonable period for the customer or consumer to opt-out of certain disclosures that shall include the following methods:

- By telephone- allow the consumer to opt out by calling a telephone number within 30 days after the date the Firm mailed the notice;
- By Mail- allow the consumer to opt out by mailing a form within 30 days after the date the Firm mailed the notice;
- By electronic means- if a customer elects to receive an electronic notice through the use of the Firm's Web site in the process of opening an account, the customer shall have thirty (30) days after the date that the customer acknowledged receipt of such notice in conjunction with the opening of the account; and
- Isolated Transaction- for isolated transactions such as the cross-offering of additional services by a broker/dealer or other financial institution, the customer shall receive the notice at the time of the transaction whereby the Firm requests the customer to decide whether to opt out before completion of the transaction.

Note: The Firm understands that it does not provide a reasonable means to opt-out if the only options for the consumer are to (1) write his or her own letter requesting to opt out; (2) to use check-off boxes provided with the initial notice but not with subsequent notices. ►►

Implementation Strategy

Not applicable. The Firm does not use an opt-out notice because it does not disclose customer information to non-affiliated third parties (except as permitted or required by law).

Exceptions to Opt-Out Requirements for Service Providers/Joint Marketing Firms

The Firm may share information with a nonaffiliated third party without providing the consumer a right to opt out if the third party is to perform services for (or functions on behalf of) the financial institution, including marketing the institution's own products or services, or financial products or services offered under a joint agreement between two or more financial institutions. However, the Firm is required to fully disclose to the consumer that it will provide this information to the nonaffiliated third party before sharing the information.

Providing Opt-Out Notification to Consumers with Non-public Personal Information

The Firm understands that it shall comply with the Rule by providing all consumers with the option to opt out disclosure of any/all personal non-public information regardless of whether the Firm has entered into a customer relationship with the customer. If the Firm has not complied with the Rule, the Firm understands that it may not disclose any personal non-public information about a consumer that may have been collected, either directly or through an affiliate, regardless of whether the Firm collected information before or after receiving the direction to opt-out from the consumer.

Partial Opt-Out Notification

In accordance with the rule, the Firm may allow a consumer to select certain sections of personal nonpublic information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

9.08 Re-disclosure and Reuse of Personal Non-Public Information

If the Firm *receives* personal non-public information provided under *Section 502(e)* of the G-L-B Act (exceptions), it may disclose the information to its affiliates or to the affiliates of the financial institution from which it received the information. The Firm may also disclose and use the information under the same type of exceptions in the ordinary course of business to carry out the activity covered by the exception under which the institution received the information. Any affiliates of the Firm may disclose and use the information, but only to the extent permissible to the Firm.

If the Firm receives personal non-public information *outside* one of the *Section 502(e)* exceptions, it may disclose the information to the following:

- Its affiliates;
- The affiliates of the financial institution that made the initial disclosure; and
- Any other person if the disclosure would be lawful if made directly by the financial institution from which the information was received.

If a third party receives information from the Firm outside one of the *Section 502(e)* exceptions, the third party may disclose to its affiliates or to the affiliates of the Firm. The third party also may disclose to any other person if the disclosure would be lawful if made by the broker-dealer, fund, or registered adviser. The third party's affiliates may disclose and use the information to the same extent permissible for the third party.

9.09 Safeguarding Customer Information

In accordance with SEC Rule 30 of Regulation S-P, the Firm has adopted certain policies and procedures that address the administrative, technical, and physical safeguards for the protection of customer information. These policies and procedures are designed to insure the security and confidentiality of customer records and information, protect against anticipated threats or hazards as well as unauthorized access to customer records or information that may result in harm or inconvenience to a customer.

Wireless Fidelity (Wi-Fi)

While Wi-Fi is a generic term used to refer to various types of wireless networks, it often refers to wireless connectivity to the Internet. This connectivity can take several forms. For example, many people have wireless capabilities in their homes, and some telecommunications vendors now offer wireless Internet connectivity that is as broad-based as cell phone coverage, which can allow people to connect wirelessly to the Internet from anywhere within the coverage area. However, data broadcast out into the airwaves makes any confidential information in that data easier to intercept than if the user is required to tap into a physical wire. Additionally, wireless connections present an attractive mechanism for hackers to tap into the user's workstation to gain access to a corporate network. A corporate network's protective measure (*e.g.*, firewalls and similar defensive software) could be by-passed under such circumstances because, when a user connects a workstation directly to the Internet, the workstation itself becomes the connection point, without the benefit of all the protections available to a corporate network. Every workstation connected directly to the Internet creates a separate opportunity for intrusion. Wi-Fi users can mitigate the risks of this intrusion by, for example, having the same or similar types of protections installed locally in the workstation that a corporate network provides.

Due Diligence for Outsourcing Arrangements

In addition to the implementation strategy for outsourced functions outlined in section 3.22, the Firm's designated supervisor will include a review of a third-party vendor's ability to ensure confidentiality of customers information, where applicable.

Remote Access

Remote access to corporate networks through VPNs or other technology may raise similar concerns. While some employees may use wireless connections, others access corporate networks remotely through physical wire connections. Physical connections to corporate networks present similar concerns as Wi-Fi connections, although members can more easily address some of these concerns through the use of firewalls, routers, filters, and other means to guard against intrusion. Before permitting associated persons to access customer information remotely, members must implement appropriate measures to secure the customer information. (NTM 05-49; Jul. 28, 2005)

Implementation Strategy

The Firm's designated supervisor will review and maintain the Firm's existing policies with respect to safeguarding customer records and information. In the event the Firm permits the use of Wi-Fi technology, or permits its customers to provide certain information to the Firm through an existing website in order to view account activity or otherwise conduct transactions, at a minimum, the Firm's designated supervisor will ensure the use of appropriate safeguards such as the use of 128-bit Secure Socket Layer (SSL) encryption security with passwords to ensure a safe transmission of data between the Firm and its customers to help prevent unauthorized parties from accessing data. Otherwise, all information provided by customers is stored and transmitted in a secure environment, accessible only by a select group of people who are given secure pass codes to access such information. In the event the Firm permits the use of Remote Access, the Firm will employ the use of necessary firewalls, routers, filters and other means to guard against intrusion.

Cloud-based Email Account Takeovers

FINRA reminds member firms that, under the Regulation S-P, they are required to have policies and procedures that address the protection of customer information and records. This includes protecting 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.

Attackers have executed email account takeovers (ATOs) at member firms using techniques such as:

- phishing emails that impersonated support personnel requesting log-in credentials;
- credential stuffing, where the attackers automatically enter previously breached credentials into various websites and applications until they successfully match to an existing account;
- stolen passwords from a user's personal email account; and
- "brute-force attacks," where the attackers submit a large number of potential passwords until one of them works.

Following execution of the email ATO, the attacker may:

- email back-office personnel asking about wire transfers and other money movement procedures, or instructing them to transfer funds to a fraudulent external bank account;
- email firm clients instructing them to transfer funds to a fraudulent external bank account;
- install malware that creates a new avenue for attackers to access the users' accounts; or
- forward client information to another email account.

Preventing ATOs

Firms are encouraged to take the following steps to configure their cloud-based email environments to help address possible ATO attacks:

- **2FA** – Implemented 2FA for all email account log-in activity outside of the firm's network for general users (e.g., for registered representatives and, internal administrators). On the O365 platform, some firms also implemented 2FA for Microsoft Partners and used the Microsoft

Authenticator application on users' mobile devices or a dynamically generated personal identification number (PIN) sent via SMS text to provide the second factor.

- **Email Archiving** – Retained and archived all emails in a separate location from the email server to provide the firm with an additional copy of all inbound and outbound emails. In addition, some firms implemented alerts to appropriate firm personnel if there were interruptions in email archiving services.
- **Logs** – Maintained and retained logs of all email account access for an adequate period of time.
- **Administrator Accounts** – Carefully managed all firm administrator accounts by:
    - closely supervising which individuals received administrator accounts to limit access to specifically authorized individuals and minimize the number of individuals with such accounts;
    - reviewing the level of access granted to administrator accounts;
    - monitoring administrator accounts' activities, especially those of "global admin" accounts; and
    - on the O365 platform, confirming administrative privileges delegated to Microsoft Partners and evaluating whether Microsoft Partners should receive "full admin" rights or if "limited admin" privileges are sufficient

Responding to ATOs

Firms should consider one or more of the following response measures for ATOs:

- immediately shutting down the email account by disabling access or resetting the compromised email account with a sufficiently complex password prior to reinstating the account;
- evaluating whether appropriate forensic expertise was available within the firm or whether a third-party service provider should be hired;
- making a copy of any affected email account, including all emails across all folders (such as those hosted by the record retention provider) to capture all information potentially accessed by the attacker at the time of the compromise;
- reviewing all of the email content in the compromised account, including attachments, to determine whether the attacker had access to sensitive or confidential information, such as PII;
- determining whether any client information was breached and notification required under federal or state law;
- confirming that any malware or viruses were deleted and unnecessary user accounts were closed;
- reviewing the overall cybersecurity environment to address any other potential impacts of the attack;
- implementing 2FA controls, if not already in use; and
- notifying appropriate law enforcement agencies (e.g., the local Federal Bureau of Investigation field office) and their FINRA Regulatory Coordinator of the attack. (Information Notice 10/02/19; Publish Date: October 2, 2019)

Implementation Strategy

The designated supervisor will review the Firm's existing policies with respect to safeguarding customer records and information. Regarding cloud-based email environments, the Firm's Safeguarding measures will include one or more of the following:

- use of two factor authentication (2FA) for all email account log-in activity outside of the firm's network for general users.
- Email Archiving in a separate location from the email server to provide the firm with an additional copy of all inbound and outbound emails.
- Maintain logs of email account access.
- Manage Administrator Accounts

In the event the Firm experiences an email account takeover (ATO), the Firm will respond

by implementing some or all of the following based on the facts and circumstances of the incident:

- immediately shutting down the email account by disabling access or resetting the compromised email account with a sufficiently complex password prior to reinstating the account;
- evaluating whether appropriate forensic expertise was available within the firm or whether a third-party service provider should be hired;
- making a copy of any affected email account, including all emails across all folders (such as those hosted by the record retention provider) to capture all information potentially accessed by the attacker at the time of the compromise;
- reviewing all of the email content in the compromised account, including attachments, to determine whether the attacker had access to sensitive or confidential information, such as PII;
- determining whether any client information was breached and notification required under federal or state law;
- confirming that any malware or viruses were deleted and unnecessary user accounts were closed;
- reviewing the overall cybersecurity environment to address any other potential impacts of the attack;
- implementing 2FA controls, if not already in use; and
- notifying appropriate law enforcement agencies (e.g., the local Federal Bureau of Investigation field office) and their FINRA Regulatory Coordinator of the attack