MAY 2, 2019

Safe and Sound - FINRA and the SEC Issue Guidance on Handling Customer Information and Communications

For more information, contact:

Patricia Jo
+1 212 556 2376
pjo@kslaw.com

Richard Margolies
+1 212 827 4080
rmargolies@kslaw.com

Mirella A. deRose
+1 212 827 4083
mderose@kslaw.com

Russ Ryan
+1 202 626 5457
rryan@kslaw.com

Michael J. Watling
+1 212 827 4082
mwatling@kslaw.com

Russell Johnston
+1 212 827 4081
rjohnston@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

Recently, the Financial Industry Regulatory Authority ("FINRA") and the SEC's Office of Compliance Inspections and Examinations ("OCIE") separately issued important guidance regarding customer communications surrounding the departure of a registered representative and customer privacy issues, respectively:

- On April 5, 2019, FINRA issued Regulatory Notice 19-10 ("Reg. Notice 19-10") addressing member firms' responsibilities when communicating with customers about departing registered representatives.[1] Reg. Notice 19-10 provides instruction to member firms regarding their obligation to promptly and clearly answer customer questions pertaining to such departures, so that customers have the ability to make timely and informed decisions about where to maintain their assets; and
- On April 16, 2019, OCIE published a Risk Alert (the "OCIE Alert") providing a list of common violations related to Regulation S-P, the primary SEC rule protecting the privacy of customer information.[2]

Taken together, these notices remind broker-dealers that customers come first, especially when it comes to safeguarding customer information and ensuring that customers are positioned to make informed decisions about their investments. This client alert focuses on key takeaways from Reg. Notice 19-10 and the OCIE Alert, and outlines best practices for broker-dealer compliance with customer communication and privacy regulations.

CUSTOMER COMMUNICATIONS WHEN A REGISTERED REPRESENTATIVE DEPARTS A FIRM

FINRA's Reg. Notice 19-10 addresses the frequent movement of registered representatives between firms, and the corresponding need for firms to provide customers with timely disclosure of key information upon a representative's departure. Reg. Notice 19-10 directs firms to provide "timely and complete answers, if known, to all customer questions resulting from a departing representative, so that customers may make informed decisions about their accounts."[3] Interestingly, this notice comes at a time when several large firms have announced they are leaving the Broker Recruiting Protocol, which allows registered representatives to maintain possession of a limited amount of customer information, such as customer names and contact information, when they move between member firms.[4] FINRA's notice serves to remind member firms that regardless of industry protocols governing broker recruiting, each firm is obligated to "promptly and clearly communicate to affected customers how their accounts will continue to be serviced" should those customers choose to remain at the firm, and to "provide customers with timely and complete answers" about the departing representative even when they wish to transfer their accounts to the representative's new firm.[5]

These disclosure obligations ensure that customers will not experience an "interruption in service" as a result of their broker's departure, and require firms to put in place "policies and procedures reasonably designed to assure that the customers serviced by that [departing] registered representative are aware of how the customers' account will be serviced at the member firm, including how and to whom the customer may direct questions and trade instructions following the representative's departure, and if and when assigned, the representative to whom the customer is now assigned at the member firm."[6]

Reg. Notice 19-10 requires transparency and timeliness in response to customer inquiries and provides the following guidance:

- Member firm "should communicate clearly, and ***without obfuscation***, when asked questions by customers about the departing registered representative" (emphasis added);
- Notwithstanding privacy and legal requirements, the firm's communications may include, when asked by a customer: (1) that the customer has the choice to retain assets at the current firm and be served by a newly assigned representative, or to transfer assets to another firm; and (2) provided that the departing representative consented to disclosure of his or her contact information, reasonable contact information (i.e. phone number, email, mailing address) of the departing representative; and
- Information provided to customers must be "fair, balanced, and not misleading."[7]

Notably, Reg. Notice 19-10 does not require firms to obtain the contact information of the departing representative if it is not known by those responsible for reassigning and continuing to service the account at the time of the customer's question. With that in mind, firms should consider implementing written policies and procedures that provide all departing representatives the opportunity to leave their contact information when exiting a firm. Firms should also consider establishing, if not already in place, written policies and procedures that address the following:

- The opportunity for departing employees to provide reasonable contact information and consent for the firm to share this contact information with their existing customers;
- The manner in which the firm will make timely and sufficient disclosures to the customers of a departing representative so that those customers can make informed choices as to whether to keep their assets at the firm or transfer them to another firm, without interruption to service;
- The identification of a point-person for handling customer inquiries regarding departed representatives; and

- The creation of a re-assignment policy for customer accounts when a registered representative leaves the firm, so that those accounts can continue to be serviced while the customer decides whether to maintain said accounts at the firm.

Such policies should be updated annually, implemented uniformly, and made available to all customers upon the commencement of their relationship with the firm.

MAINTAINING CUSTOMER PRIVACY PURSUANT TO REGULATION S-P

Over the last several years, FINRA and the SEC have been focused on safeguarding customer information in light of heightened cybersecurity risks.[8] Key protections include Rule 30 of the SEC's Regulation S-P, which requires that "[e]very broker, dealer . . . adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[9] In addition, Rule 201 of Regulation S-ID (the "Identity Theft Red Flags Rule") requires that broker-dealers create and implement written identity theft prevention programs "designed to detect, prevent, and mitigate identity theft."[10]

The OCIE Alert highlights common violations by registrants and serves as a warning to firms that cybersecurity and privacy controls will be a focus of examination.[11] Specifically, the OCIE Alert addresses issues related to Regulation S-P's "Safeguards Rule," which requires registrants to: (1) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices generally no later than when it establishes a customer relationship ("Initial Privacy Notice"); (2) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship ("Annual Privacy Notice," and together with the Initial Privacy Notice, "Privacy Notices"); and (3) deliver a clear and conspicuous notice to its customers that accurately explains the right to opt out of some disclosures of non-public personal information of the customer to nonaffiliated third parties ("Opt-Out Notice").[12]

The OCIE Alert helpfully details the compliance weaknesses identified most frequently by OCIE staff in connection with the above rule:

- Failure to provide Initial Privacy Notices, Annual Privacy Notices, and Opt-Out Notices to customers;[13]
- Failure to have written privacy policies and procedures as required by the rule;
- Failure to implement existing written policies;
- Policies and procedures that were not reasonably designed to safeguard customer records and information, including instances where:
  - Policies failed to address how personal devices, like cell phones, should be configured to safeguard customer information;
  - Policies failed to prevent employees from sending unencrypted emails to customers containing "personally identifiable information" or "PII;"[14]
  - Employees were not given training on the use of encryption, passwords, and other protected methods of transmitting customer information;
  - Policies were not in place to prohibit employees from sending customer PII to unsecured locations outside of the registrants' networks;
  - Policies concerning privacy and data protection were not applied to outside vendors that handled customer PII, even where such policies were in place;

- Policies failed to identify all systems on which customer PII would be maintained;
- Customer PII was stored in unsecured physical locations, such as unlocked file cabinets in open offices;
- Customer login credentials were shared with more employees than permitted under the firm's policies and procedures; and
- Registrants failed to rescind departed employees' access rights to restricted customer information, and those employees were able to access such information after their departure.[15]

The vulnerabilities discussed above highlight the need for firms to implement policies and procedures to ensure both the safeguarding of customer information and that customers are informed as to how and by whom their information may be used.

CONCLUSION

Broker-dealers should interpret FINRA's Reg. Notice 19-10 and OCIE's Risk Alert together as a timely opportunity to review written policies and procedures, which must be reasonably designed to ensure: proper communication of information to customers during the course of the customer relationship and upon the departure of financial advisors; and the safeguarding of customer records and information, including protection against unauthorized access to internal firm systems and the information maintained therein.

[1] FINRA, Regulatory Notice 19-10, *Customer Communications* (April 5, 2019), *available at* https://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-19-10.pdf.

[2] SEC, Office of Compliance Inspections and Examinations Risk Alert, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies* (April 16, 2019), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

[3] *See* FINRA, Regulatory Notice 19-10, at 2, *supra* note 1.

[4] Created in 2004, the Broker Recruiting Protocol currently has over 1,800 signatories and allows for registered representatives to take with them the client name, address, phone number, email address, and account title of each client they serviced while at the firm. The protocol was established to reduce litigation stemming from the departure of registered representatives. *Available at* Carlile Patchen & Murphy LLP, www.thebrokerprotocol.com/index.php/faqs (last visited April 30, 2019).

[5] *See* FINRA, Regulatory Notice 19-10, at 1, *supra* note 1.

[6] *Id.* at 2.

[7] *Id.* at 3.

[8] In 2017, the SEC's Division of Enforcement created a specialty Cyber Unit and in 2018, brought its first case against a firm for the violation of Regulation S-ID, known as the Identity Theft Red Flags Rule, in relation to a cyber intrusion incident. *See* SEC, Division of Enforcement 2018 Annual Report, at 7 *available at* https://www.sec.gov/files/enforcement-annual-report-2018.pdf (the SEC also charged the firm for violating Regulation S-P). FINRA has also continued to make cybersecurity a priority for its exam and enforcement programs. In its most recent exam priorities letter, FINRA stated that it would focus on the adequacy of firms' cybersecurity programs to protect sensitive information, including customer PII. *See* FINRA, *2019 Risk Monitoring and Examination Priorities Letter* (Jan. 2019), *available at* https://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf. Additionally, in December 2018, FINRA published a report outlining best practices for cybersecurity controls in light of the increasingly sophisticated and evolving cybersecurity risks and challenges faced by broker-dealer firms. *See generally* FINRA, *Report on Selected Cybersecurity Practices -2018* (Dec. 2018), *available at* http://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

[9] 17 C.F.R. § 248.30 (2019) ("These written policies and procedures must be reasonably designed to: (1) Insure the security and confidentiality of customer records and information; (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.").

[10] 17 C.F.R. § 248.201 (2019) ("Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.").

[11] SEC, Office of Compliance Inspections and Examinations Risk Alert, *supra* note 2.

[12] *Id.*

[13] *Id.* This includes instances when firms sent notices to customers that did not accurately reflect the firm's policies and procedures, and when they did not provide notice to customers of their right to opt out of the registrant sharing their non-public personal information with nonaffiliated third parties.

[14] *Id.* at 3. As defined in 2 C.F.R. § 200.79 (2019), PII means "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."

[15] *See,* SEC, Office of Compliance Inspections and Examinations Risk Alert, *supra* note 2.