NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")[1]

Volume IV, Issue 4 **February 3, 2015**

This Risk Alert provides summary observations from OCIE's examinations of registered broker-dealers and investment advisers, conducted under the Cybersecurity Examination Initiative, announced April 15, 2014.

CYBERSECURITY EXAMINATION SWEEP SUMMARY

I. Introduction

OCIE's National Examination Program staff (the "Staff"), recently examined 57 registered broker-dealers and 49 registered investment advisers to better understand how broker-dealers and advisers address the legal, regulatory, and compliance issues associated with cybersecurity (the "Cybersecurity Examination Initiative" or the "Initiative").[2] The examined firms were selected to provide perspectives from a cross-section of the financial services industry and to assess various firms' vulnerability to cyber-attacks. Appendices A and B include breakdowns of the types of broker-dealers and advisers examined.

In the examinations, the staff collected and analyzed information from the selected firms relating to their practices for: identifying risks related to cybersecurity; establishing cybersecurity governance, including policies, procedures, and oversight processes; protecting firm networks and information; identifying and addressing risks associated with remote access to client information and funds transfer requests; identifying and addressing risks associated with vendors and other third parties; and detecting unauthorized activity. In addition to reviewing documents, the staff held interviews with key personnel at each firm regarding its: business and operations; detection and impact of cyber-attacks; preparedness for cyber-attacks; training and policies relevant to cybersecurity; and protocol for reporting cyber breaches.[3]

The staff's document reviews and questions were designed to discern basic distinctions among the level of preparedness of the examined firms. The staff conducted limited testing of the

---

1 The views expressed herein are those of the staff of OCIE, in coordination with other staff of the Securities and Exchange Commission ("SEC" or "Commission"), including the Division of Trading and Markets and the Division of Investment Management. The Commission has expressed no view on the contents of this Risk Alert. This document was prepared by the SEC staff and is not legal advice.

2 *See* OCIE, "OCIE Cybersecurity Initiative" (April 15, 2014), available at: http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

3 The Initiative's review period for broker-dealers covered calendar year 2013; adviser examinations, which began a few months after the broker-dealer examinations, reviewed firm practices in 2013 through April 2014.

accuracy of the responses and the extent to which firms' policies and procedures were implemented. The examinations did not include reviews of technical sufficiency of the firms' programs.

This Risk Alert provides summary observations from the examinations conducted under the Cybersecurity Examination Initiative.

II. Summary Examination Observations

- *The vast majority of examined broker-dealers (93%) and advisers (83%) have adopted written information security policies.* Most of the broker-dealers (89%) and the majority of the advisers (57%) conduct periodic audits to determine compliance with these information security policies and procedures.

    - *Written business continuity plans often address the impact of cyber-attacks or intrusions.* Such written policies and procedures, for both the broker-dealers (82%) and the advisers (51%), discuss mitigating the effects of a cybersecurity incident and/or outline the plan to recover from such an incident.

    - *Written policies and procedures generally do not address how firms determine whether they are responsible for client losses associated with cyber incidents.* The policies and procedures of only a small number of the broker-dealers (30%) and the advisers (13%) contain such provisions, and even fewer of the broker-dealers (15%) and the advisers (9%) offered security guarantees to protect their clients against cyber-related losses.

    - *Many firms are utilizing external standards and other resources to model their information security architecture and processes*. Most of the broker-dealers (88%) and many of the advisers (53%) reference published cybersecurity risk management standards, such as those published by the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), and the Federal Financial Institutions Examination Council ("FFIEC").

- *The vast majority of examined firms conduct periodic risk assessments, on a firm-wide basis, to identify cybersecurity threats, vulnerabilities, and potential business consequences*. These broker-dealers (93%) and advisers (79%) reported considering such risk assessments in establishing their cybersecurity policies and procedures.

    - *Fewer firms apply these requirements to their vendors.* A majority of the broker-dealers (84%) and approximately a third of the advisers (32%) require cybersecurity risk assessments of vendors with access to their firms' networks.

- *Most of the examined firms reported that they have been the subject of a cyber-related incident.* A majority of the broker-dealers (88%) and the advisers (74%) stated that they

have experienced cyber-attacks directly or through one or more of their vendors. The majority of the cyber-related incidents are related to malware and fraudulent emails.

- Over half of the broker-dealers (54%) and just under half of the advisers (43%) reported receiving fraudulent emails seeking to transfer client funds. Over a quarter of those broker-dealers (26%) reported losses related to fraudulent emails of more than $5,000; however, no single loss exceeded $75,000. One adviser reported a loss in excess of $75,000 related to a fraudulent email, for which the client was made whole.

- One-quarter (25%) of the broker-dealers that had losses related to fraudulent emails noted that these losses were the result of employees not following the firms' identity authentication procedures. The one adviser that reported a loss also noted that its employees had deviated from its identity authentication procedures.

- Almost two-thirds of the broker-dealers (65%) that received fraudulent emails reported the emails to the Financial Crimes Enforcement Network (FinCEN) by filing a Suspicious Activity Report (SAR),[4] but only a small number of those firms reported the fraudulent emails to law enforcement or other regulatory agencies (7%). With the exception of the investment adviser loss in excess of $75,000 related to a fraudulent email noted above, advisers generally did not report incidents to a regulator or law enforcement.

- While firms identified misconduct by employees and other authorized users of the firms' networks as a significant concern, only a small proportion of the broker-dealers (11%) and the advisers (4%) reported incidents in which an employee or other authorized user engaged in misconduct resulting in the misappropriation of funds, securities, sensitive client, or firm information, or in damage to the firms' networks.

- *Many examined firms identify best practices through information-sharing networks.* Almost half of the broker-dealers (47%) were members of industry groups, associations, or organizations (both formal and informal) that exist for the purpose of sharing information regarding cybersecurity attacks and identifying effective controls to mitigate harm. Many of the broker-dealers identified the Financial Services Information Sharing

[4] *See* 31 C.F.R. § 1023.320(a)(2). Broker-dealers are obligated to report a transaction involving funds or other assets of at least $5,000 that is conducted or attempted by, at, or through the firm if the firm knows, suspects, or has reason to suspect, in part, that the transaction involves use of the broker-dealer to facilitate criminal activity. The scope of these particular exams did not include a review of the broker-dealers' compliance with this rule.

and Analysis Center ("FS-ISAC") as adding significant value in this effort. While a few of the advisers also identified FS-ISAC as a resource, advisers more frequently relied on discussions with industry peers, attendance at conferences, and independent research to identify cybersecurity practices relevant to their business and learn about latest guidance from regulators, government agencies, and industry groups.

- *The vast majority of examined firms report conducting firm-wide inventorying, cataloguing, or mapping of their technology resources*. Such practices were reportedly performed for the following devices, systems, and resources at the broker-dealers and advisers, respectively: physical devices and systems (96% and 92%); software platforms and applications (91% and 92%); network resources, connections, and data flows (97% and 81%); connections to firm networks from external sources (91% and 74%); hardware, data, and software (93% and 60%); and logging capabilities and practices (95% and 68%).

- *The examined firms' cybersecurity risk policies relating to vendors and business partners revealed varying findings.* Most of the broker-dealers incorporate requirements relating to cybersecurity risk into their contracts with vendors and business partners (72%). In contrast, few of the advisers incorporate such requirements (24%). Similarly, a slim majority of the broker-dealers maintain policies and procedures related to information security training for vendors and business partners authorized to access their networks (51%), whereas a much smaller number of the advisers have such policies (13%).

- *Almost all the examined broker-dealers (98%) and advisers (91%) make use of encryption in some form*.

- *Many examined firms provide their clients with suggestions for protecting their sensitive information.* Of the broker-dealers with retail customers that offer online access (65%), all firms (or their clearing firms or third-party vendors) provide their customers with some form of information about reducing cybersecurity risks in conducting transactions with the firm. Similarly, of the advisers that primarily advise retail clients and permit those clients to access their account information on-line (26%), the majority (75%) provide those clients with information about certain steps that can be taken to reduce cybersecurity risks when conducting business with the firm. The information may be directly addressed to clients on the advisers' website or in periodic email or postal distributions (*i.e.*, newsletters or bulletins).

- *The designation of a Chief Information Security Officer ("CISO") varied by the examined firms' business model.* Approximately two-thirds of the broker-dealers (68%) examined have an individual explicitly assigned as the firm's CISO. In contrast, less than a third of the advisers (30%) have designated a CISO; rather, the advisers often direct

their Chief Technology Officer to take on the responsibilities typically performed by a CISO or they have assigned another senior officer (*i.e.*, the Chief Compliance Officer, Chief Executive Officer, or Chief Operating Officer) to liaise with a third-party consultant who is responsible for cybersecurity oversight.

- *Use of cybersecurity insurance revealed varying findings among the examined firms.* Over half of the broker-dealers maintain insurance for cybersecurity incidents (58%). In contrast, a small number of the advisers (21%) maintain insurance that covers losses and expenses attributable to cybersecurity incidents. Out of the broker-dealers and advisers, only one broker-dealer and one adviser reported that they had filed claims.

III. Conclusion

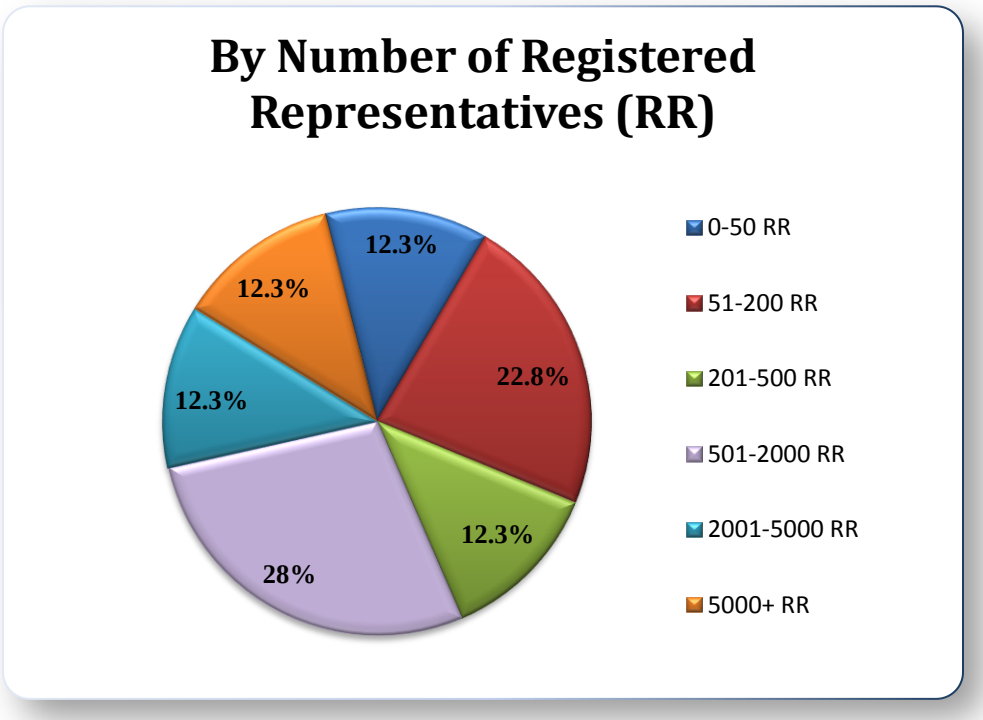
The staff is still reviewing the information to discern correlations between the examined firms' preparedness and controls and their size, complexity, or other characteristics. As noted in OCIE's 2015 priorities, OCIE will continue to focus on cybersecurity using risk-based examinations.[5]

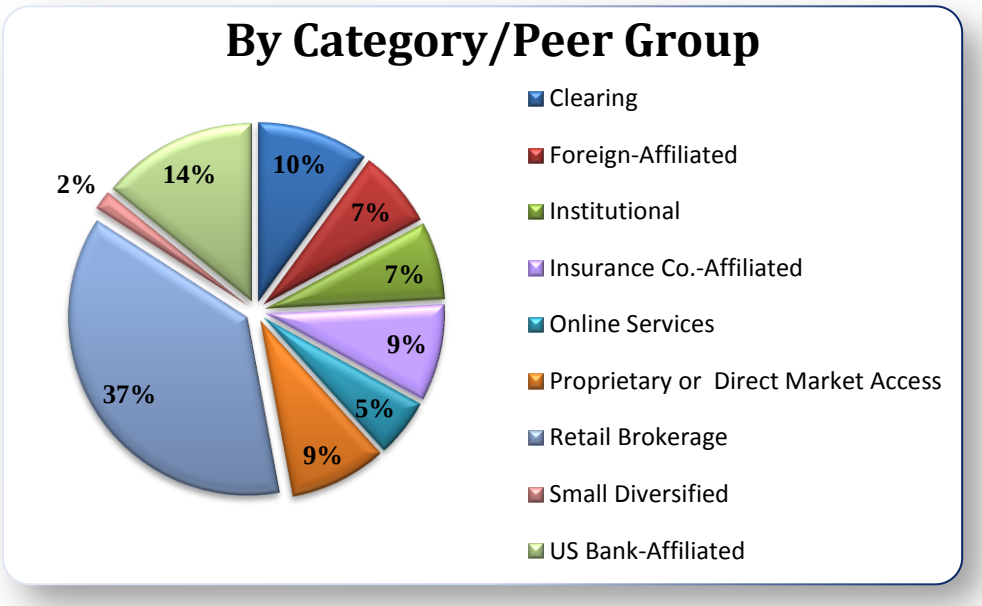
The Staff welcomes comments and suggestions about how the Commission's examination program can better fulfill its mission to promote compliance, prevent fraud, monitor risk, and inform SEC policy. If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify us at http://www.sec.gov/complaint/info_tipscomplaint.shtml.

This Risk Alert is intended to highlight for firms risks and issues that the Staff has identified in the course of examinations of broker-dealers' and investment advisers' controls regarding cybersecurity and preparedness. In addition, this Risk Alert describes factors that firms may consider to (i) assess their supervisory, compliance and/or other risk management systems related to cybersecurity risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. These factors are not exhaustive, nor will they constitute a safe harbor. Factors other than those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business. While some of the factors discussed in this Risk Alert reflect existing regulatory requirements, they are not intended to alter such requirements. Moreover, future changes in laws or regulations may supersede some of the factors or issues raised here. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[5] OCIE, "Examination Priorities for 2015" (Jan. 13, 2015), *available at*: http://www.sec.gov/news/pressrelease/2015-3.html.

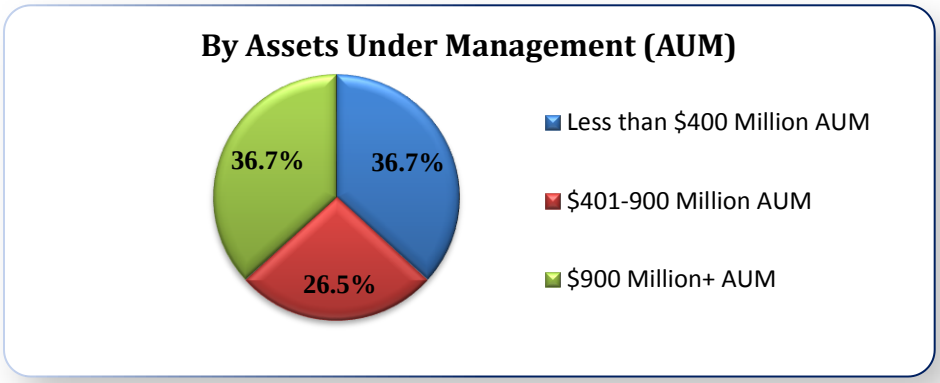
Appendix A – Breakdown of Examined Broker-Dealers[6]

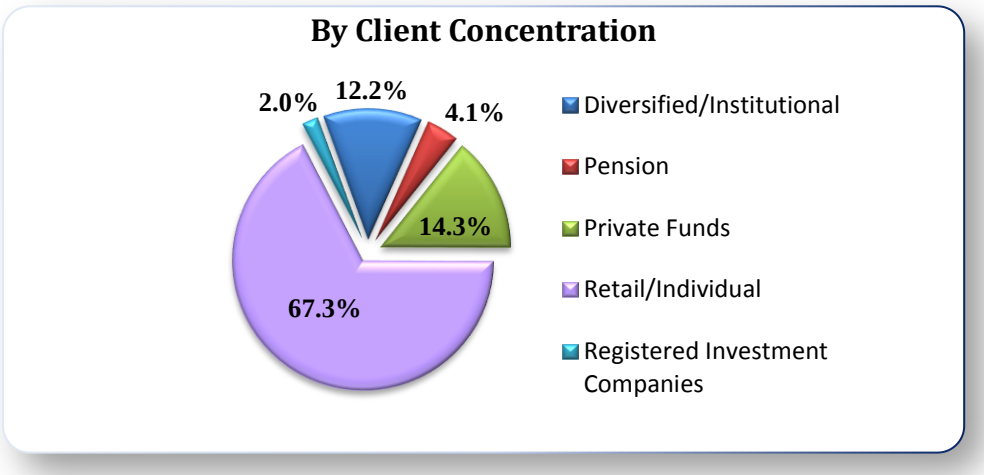


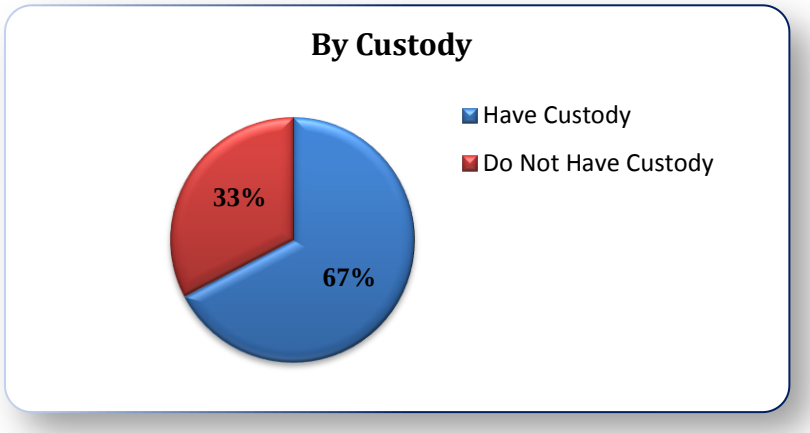


[6] Figures in this Appendix are rounded approximations.

Appendix B – Breakdown of Examined Investment Advisers[7]







[7] Figures in this Appendix are rounded approximations.