Utah Division of Securities Investment Adviser Examination Guide

Introduction

The Utah Division of Securities (the "Division") is conducting a focused examination of all Utah state-covered registered investment advisers ("RIA") currently licensed to transact business in the state of Utah. A signed Examination Submission Form will be **due on or before thirty (30) days from the date on your Examination Cover Letter**. This is a requirement to successfully complete the exam.[1] All responses reflect the RIA firm's circumstances as of the date of its examination submission.

Information provided in this examination is to educate RIA business owners, its designated officials, and its investment adviser representatives ("IAR"). **The material in this examination is not to be considered legal, compliance consulting, or business consulting advice.**

The Division, as a Utah State government entity, is unable to act in the following capacities for any RIA firm:

- To act in the capacity of a person or entity's private business legal adviser, counsel, or otherwise.
- To act in the capacity or in place of a person or entity's private business regulatory compliance officer or consultant.
- To act as a person or entity's private business consultant.

Operating a compliant securities business is the responsibility of the RIA business owner(s), designated officials, and licensed or unlicensed employees. ***Persons or entities cannot shift the burden of individual or entity compliance to the Division.***

The Division will use the North American Securities Administers Association ("NASAA") Cybersecurity Checklist ("Checklist") as the guide for instruction and examination questions. NASAA represents state and provincial securities regulators in the United States, Canada, and Mexico. The Division is a NASAA member.

---

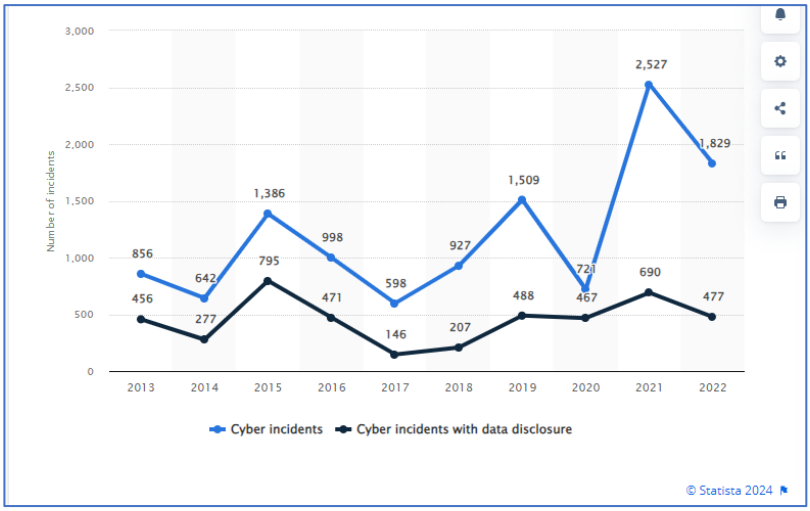
[1] **Answer is required**: The Utah Division of Securities conducts this examination under authority granted in § 61-1-5 of the Utah Uniform Securities Act (UUSA). Participation in this examination is required, as a failure to comply with a request made pursuant to UUSA § 61-1-5 constitutes a dishonest or unethical business practice in accordance with Rule 164-6-1g(E)(23) of the Utah Administrative Code (UAC).

Both the full Checklist items and the subset of Checklist items that will make up the examination questions are identified in this instruction guide. **Again, submit responses to the examination questions only on the Examination Submission Form.** Answer all questions truthfully and completely. It is unlawful to make a false or misleading statement in this examination.[2]

Why is the Division focusing on Cybersecurity for Utah state-covered RIAs?

It is obvious to anyone who sends emails, navigates e-commerce platforms, or exchanges data via a smartphone that protecting yourself in a digital world is a necessity.

However, businesses that handle other people's money must be particularly vigilant. Below is a chart of the number of cyber incidents in the financial industry worldwide from 2013 to 2022. The financial industry is consistently one of the most targeted for cyber attacks.

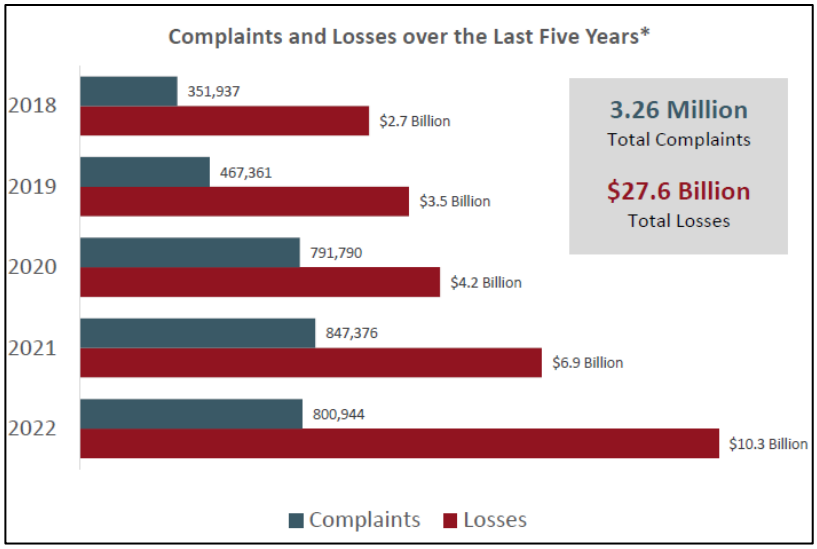


According to the FBI, the growth of cyber complaints and personal losses due to cyber complaints have exploded over the last five years.[3]

---

[2] UUSA § 61-1-5 and § 61-1-16. It is unlawful to make any statement that is false or misleading (including omissions that mislead) in any material respect in examination documents filed with the Division. Which, for the purposes of this examination, includes the answers to examination questions on the Examination Submission Form.

[3] 2022 FBI Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.



The Division is not the only regulator focusing on cybersecurity. The Securities and Exchange Commission ("SEC") is aggressively addressing the issue by working for almost two years on new cybersecurity regulations. The "Cybersecurity Risk Management" rule is expected to be finalized in 2024.[4] The fact sheet in the Appendix states that the new SEC rule will require additional documentation of your firm's cybersecurity risk management processes in the Written Supervisory Procedures ("WSP") or Policies and Procedures Manual ("P&P"). Additional disclosures related to cybersecurity risks and incidents, and adding additional books and records requirements are also proposed. Also, there are new due diligence requirements firms must conduct when selecting vendors to provide IT services.

A second SEC proposed rule impacting cybersecurity involves "Proposed Enhancements to Regulation S-P".[5] The SEC adopted Regulation S-P ("Reg S-P") to address financial service firms' handling of a client's protected personal

[4] *See Appendix A* Cybersecurity Risk Management Fact Sheet for an overview on the proposed rule. Additional information on the proposed rule is available at "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies", https://www.sec.gov/rules/2022/02/cybersecurity-risk-management-investment-advisers-registered-investment-companies-and#33-11028. While these rules have not been finalized, your firm should understand the additional regulations that are pending and your firm's obligation to follow all final regulations.

[5] *See Appendix B* for the Fact Sheet on "Proposed Enhancements to Regulation S-P" and additional information at. https://www.sec.gov/rules/2023/03/regulation-S-P-privacy-consumer-financial-information-and-safeguarding-customer. In March 2023, the SEC issued Proposed Enhancements to Regulation S-P for financial institutions including investment advisers. While these rules have not been finalized, your firm should understand the additional regulations that are pending and your firm's obligation to follow all final regulations.

information ("PPI").[6] Reg S-P privacy regulations have been in place since the early 2000s, with regular updates. It identifies collecting, safeguarding, sharing, and disposing of sensitive information, including non-public information ("NPI") and PPI. Your annual privacy notice to clients is part of Reg S-P. Enhancements include documenting additional processes in the firm's WSP/P&P and broadening the scope of information covered under Reg S-P.

It is important to note that the proposed rules *expand current regulations*. Current cybersecurity risk management requirements are covered by Reg S-P, RIA books and records requirements, RIA supervision requirements, and the overall duty as a fiduciary to act in the best interest of your clients by being able to service clients and protect sensitive client information.

The NASAA Cybersecurity Checklist[7]

The NASAA checklist is divided into five areas of focus: Identify, Protect, Detect, Respond, and Recover. This examination instruction document will show all checklist items. The Examination Submission Form includes a subset of the checklist items. Examination questions were selected based on critical items, applicable RIA books and records requirements, and items that can quickly be implemented by your RIA business.

Identify: Risk & Management

A major focus of cybersecurity regulation is for each RIA firm to have processes stating how it will operate its business to protect client assets and manage its cybersecurity risks. It is not sufficient to just complete cybersecurity practices. The practices are to be documented in the books and records of the firm as part of the firm's WSPs or P&P manuals. Annually, it is a regulatory requirement for RIA's to update its WSP or P&P documents for clarification and changes to firm operations.[8] If you need to update your policies and procedures for

---

[6] Reg S-P identifies what is considered private information. Items like social security numbers, suitability information, account balances, and even private data is obtained through internet cookies. More information on Reg S-P can be found at https://www.sec.gov/rules/2000/06/privacy-consumer-financial-information-regulation-S-P.

[7] *See Appendix C* for the complete NAASAA checklist.

[8] The Utah Uniform Securities Act incorporates by reference the books and records requirements identified under §275.204-2 of the Investment Advisers Act of 1940. *See Appendix D* for §275.204-2 and specifically, §275.204-2 (a) (17) which addresses annual policies and procedures books and records requirements. Additionally, Section §275.206 (4)-7, "Compliance Procedures and Practices," cites the mandatory requirement.

cybersecurity, this checklist will give you suggestions on what to include in your firm's compliance manual.

Being aware of the physical locations of your firm's digital devices, identifying the custodians of the devices, documenting the licensed software used by the firm and who holds the user licenses are all fundamental for managing your firm's cybersecurity risks and protecting client privacy.

Full Checklist

Identify: Risk Assessments & Management
1. Risk assessments are conducted frequently (e.g. annually, quarterly).
2. Cybersecurity is included in the risk assessment.
3. The risk assessment includes a review of the data collected or created, where the data is stored, and if the data is encrypted.
4. Internal "insider" risk (e.g. disgruntled employees) and external risks are included in the risk assessment.
5. The risk assessment includes relationships with third parties.
6. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices (e.g. frequent password changes, locking of devices, reporting of lost or stolen devices, etc.).
7. Primary and secondary person(s) are assigned as the central point of contact in the event of a cybersecurity incident.
8. Specific roles and responsibilities are tasked to the primary and secondary person(s) regarding a cybersecurity incident.
9. The firm has an inventory of all hardware and software.

Examination Questions for "Identify: Risk Assessments & Management

Identify: Risk Assessments & Management
6. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices (e.g. frequent password changes, locking of devices, reporting of lost or stolen devices, etc.).
9. The firm has an inventory of all hardware and software.

Protect: Use of Electronic Mail

The SEC adopted Reg S-P to address the safeguarding and sharing of a client's sensitive information.[9] Electronic communications are more prevalent than ever, with email being the most frequent means of written communication.

In April 2019, the SEC's Division of Examinations Risk Alert[10] addressed Reg S-P. They noted a frequent examination deficiency where firms had no "policies and procedures designed to prevent employees from regularly sending unencrypted emails with PPI". The Risk Alert further identified issues where firms had no policies or training for encryption, password-protecting documents, and transmitting communication using only registrant-approved methods.

Today, many common applications provide the ability to encrypt documents. Look at your existing software applications to determine if they offer encryption capabilities and how to use them. If necessary, you can purchase stand-alone encryption software.

Since RIA firms both send and receive email messages, an industry best practice is to educate clients on how they can encrypt digital messages they send to you. This reinforces good cybersecurity behaviors, helping to protect your clients from being a cybercrime victim. If a client message contains sensitive information (e.g. new bank information to link to his/her account, address change information, etc.), confirm the request is from the client and not someone who has taken over a client's email account before processing a request.

The industry's best practice is to send email communications securely, with or without sensitive information in the message. However, if you ever do send a message with NPI or PPI, and you are unable to send it securely, labeling the message as "unsecured" alerts the client that extra care is required to protect themselves when handling the communication. This practice should seldom be used, if ever.

---

[9] Reg S-P identifies what is considered private information. *See* footnote 6 above.

[10] *See* the SEC's Division of Examinations Risk Alert "Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies" (Apr. 16, 2019), https://www.sec.gov/ocie/announcement/ocie-risk-alert-regulation-S-P.

Full Checklist

Protect: Use of Electronic Mail
1. Identifiable information of a client is transmitted via email.
2. Authentication practices for access to email on all devices (computer and mobile devices) is required.
3. Passwords for access to email are changed frequently (e.g. monthly, quarterly).
4. Policies and procedures detail how to authenticate client instructions received via email.
5. Email communications are secured. (If the response is " NO", proceed to the next question.)
6. Employees and clients are aware that email communication is not secured.

Examination Questions for "Protect: Use of Electronic Mail"

Protect: Use of Electronic Mail
5. Email communications are secured. (If the response is " NO", proceed to the next question.)
6. Employees and clients are aware that email communication is not secure.

Protect: Devices

When a record is no longer required to be retained, it must be destroyed in a safe and secure manner. While this may seem obvious, even large firms can stumble with straightforward cybersecurity and document security. Morgan Stanley was fined $6.5m dollars in November 2023 for failing to decommission computing equipment with electronic client data.[11]

[11] *See* CNBC article "Morgan Stanley fined for putting customer personal data at risk in computer purge: New York AG", https://www.cnbc.com/2023/11/16/morgan-stanley-fined-over-computers-with-personal-data.html.

Full Checklist

Protect: Devices
1. Device access (physical and digital) is permitted for authorized users, including personnel and clients.
2. Device access is routinely audited and updated appropriately.
3. Devices are routinely backed up, and underlying data is stored in a separate location (i.e., on an external drive, in the cloud, etc.)
4. Backups are routinely tested.
5. The investment adviser has written policies and procedures regarding the destruction of electronic data and physical documents.
6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures.

Examination Questions for "Protect: Devices"

Protect: Devices
5. The investment adviser has written policies and procedures regarding the destruction of electronic data and physical documents.
6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures.

Protect: Use of Cloud Services

Cloud services are becoming the norm for data storage and access. It is inexpensive and many application and device purchases now offer free cloud storage space. Cloud storage has other advantages, including access to information across multiple devices. However, cloud storage for securities businesses comes with significant requirements. This section of the Checklist has 16 items. The takeaway is that you must know how secure your data is when it is stored using a cloud service provider. In addition, you must be aware of who and how people access data from the cloud, which requires ongoing supervision.

Records retention and retrieval are current RIA books and records requirements. It is the responsibility of the firm to retain and to be able to retrieve records for production as requested by clients and securities regulators. System data backup and storage of records at an offsite location ensures a duplicate record exists in the event that you cannot retrieve the primary record.[12]

The use of mobile electronic devices has revolutionized communications, and its proliferation is not slowing down. Investment adviser books and records requirements necessitate retaining incoming and outgoing communications, *regardless of delivery method*. In September 2022, the SEC charged 16 of the largest Wall Street firms $1.1B in fines for failing to maintain and preserve electronic communications.[13]

Since the COVID-19 pandemic, more business is being completed from remote locations than ever before. One of the ways to more securely access data stored in the cloud from a remote location is using a virtual private network ("VPN"). If you access information remotely or have concerns with using any Wi-Fi network, a VPN can add additional security. However, controls must be in place when managing VPN services for your investment adviser firm.

While not included as an examination question, the Division wants to again emphasize the SEC proposed regulations that will require rigorous due diligence of cybersecurity vendors.[14] Many questions in this checklist section will be more than good business cybersecurity practices and become regulatory requirements when the SEC proposed rules are finalized.

[12] *See Appendix D* for the books and records requirements.

[13] "SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures" (Sept. 27, 2022), SEC.GOV, https://www.sec.gov/news/press-release/2022-174.

[14] *See Appendix A* Cybersecurity Risk Management Fact Sheet.

Full Checklist

Protect: Use of Cloud Services
1. Due diligence has been conducted on the cloud service provider prior to signing an agreement or contract.
2. As part of the due diligence, the investment adviser has evaluated whether the cloud service provider has safeguards against breaches and a documented process in the event of breaches.
3. The investment adviser has a business relationship with the cloud service provider and has the contact information for that entity.
4. The investment adviser is aware of the assignability terms of the contract.
5. The investment adviser understands how the firm's data is segregated from other entities' data within the cloud service.
6. The investment adviser is familiar with the restoration procedures in the event of a breach or loss of data stored through the cloud service.
7. The investment adviser has written policies and procedures in the event that the cloud service provider is purchased, closed, or otherwise unable to be accessed.
8. The investment adviser solely relies on free cloud storage.
9. The investment adviser has a back-up of all records off-site.
10. Data containing sensitive or personally identifiable information is stored through a cloud service.
11. Data containing sensitive or personally identifiable information, which is stored through a cloud service, is encrypted.
12. The investment adviser has written policies and procedures related to the use of mobile devices by staff who access data in the cloud.
13. The cloud service provider (or its staff) may access and/or view the investment adviser's data stored in the cloud.
14. The investment adviser allows remote access to its network (e.g. through use of VPN).
15. The VPN access of employees is monitored.
16. The investment adviser has written policies and procedures related to the termination of VPN access when an employee resigns or is terminated.

Examination Questions for "Protect: Use of Cloud Services"

Protect: Use of Cloud Services
9. The investment adviser has a back-up of all records off-site.
14. The investment adviser allows remote access to its network (e.g. through use of VPN).

Protect: Use of Firm Websites

The Division is asking this examination question to learn the percentage of Utah state-covered RIA firms that have a client portal for account or non-public information access on its website. Many Utah-covered RIAs use broker-dealers or third-party money managers as client asset custodians, and their client account access is controlled and secured through these firms. If you have a client portal on your website, a careful review of checklist questions 8, and 10-13 should be completed to ensure client account records are only accessible by the client with adequate safeguards.

Full Checklist

Protect: Use of Firm Websites
1. The investment adviser relies on a parent or affiliated company for the construction and maintenance of the website.
2. The investment adviser relies on internal personnel for the construction and maintenance of the website.
3. The investment adviser relies on a third-party vendor for the construction and maintenance of the website.
4. If the investment adviser relies on a third party for website maintenance, there is an agreement with the third party regarding the services and the confidentiality of information.
5. The investment adviser can directly make changes to the website.
6. The investment adviser can directly access the domain renewal information and the security certificate information.
7. The firm's website is used to access client information.
8. SSL or other encryption is used when accessing client information on the firm's website.
9. The firm's website includes a client portal.
10. SSL or other encryption is used when accessing a client portal.
11. When accessing the client portal, user authentication credentials (i.e., username and password) are encrypted.
12. Additional authentication credentials (i.e., challenge questions, etc.) are required when accessing the client portal from an unfamiliar network or computer.
13. The investment adviser has written policies and procedures related to a denial of service issue.

Examination Question for "Use of Firm Websites"

Protect: Use of Firm Websites
9. The firm's website includes a client portal. [SURVEY QUESTION]

Protect: Custodians & Other Third-Party Vendors

Investment advisers should be aware of the way custodians of client accounts protect access to the account. How does the custodian verify the person requesting information on an account is authorized? What safeguards are available to customers in preventing unauthorized access (e.g., challenge questions, two-factor authentication, etc.)?

Full Checklist

Protect: Custodians & Other Third-Party Vendors
1. The investment adviser's due diligence on third parties includes cybersecurity as a component.
2. The investment adviser has requested vendors to complete a cybersecurity questionnaire with a focus on issues of liability sharing and whether vendors have policies and procedures based on industry standards.
3. The investment adviser understands that the vendor has IT staff or outsources some functions.
4. The investment adviser has obtained a written attestation from the vendor that it uses software to ensure customer data is protected.
5. The investment adviser has inquired whether a vendor performs a cybersecurity risk assessment or audit on a regular basis.
6. The cyber-security terms of the agreement with an outside vendor are not voided because of the actions of an employee of the investment adviser.
7. Confidentiality agreements are signed by the investment adviser and third-party vendors.
8. The investment adviser has been provided enough information to assess the cybersecurity practices of any third-party vendors.
9. [Relevant to custodians only] The investment adviser has discussed with the custodian matters regarding the impersonation of clients and authentication of client orders.

Examination Question for "Protect: Custodians & Other Third-Party Vendors"

Protect: Custodians & Other Third-Party Vendors
9. [Relevant to custodians only] The investment adviser has discussed with the custodian matters regarding the impersonation of clients and authentication of client orders.

Protect: Encryption

Encryption has already been addressed as it pertains to e-mail communications. However, while conducting normal securities business, sensitive records are retained and accessed with many other applications and devices. Data encryption of sensitive records across the enterprise is needed to meet your obligations to protect client privacy of information requirements and to safeguard sensitive RIA business books and records.

Full Checklist

Protect: Encryption
1. The investment adviser routinely consults with an IT professional knowledgeable in cybersecurity.
2. The investment adviser has written policies and procedures in place to categorize data as either confidential or non-confidential.
3. The investment adviser has written policies and procedures in place to address data security and/or encryption requirements.
4. The investment adviser has written policies and procedures in place to address the physical security of confidential data and systems containing confidential data (i.e., servers, laptops, tablets, removable media, etc.).
5. The investment adviser utilizes encryption on all data systems that contain (or access) confidential information.
6. The identities and credentials of authorized users are monitored.

Examination Question for "Protect: Encryption"

Protect: Encryption
5. The investment adviser utilizes encryption on all data systems that contain or are used to access confidential information.

Detect: Anti-Virus Protection and Firewalls

This section of the Checklist is emphasized in the Division's routine examinations. All items selected for examination questions are fundamental to cybersecurity, can generally be completed easily, and are cost-effective safeguards.

Many cybersecurity-specific programs (operating software, anti-virus software, encryption software, firewall programs, etc.) have automatic update options in the software. It is wise to set a schedule to confirm that updates are, in fact, "automatic" and have not been inadvertently turned off.

Other software programs, web browsers, mobile devices, etc. are also updated frequently. Many updates include security patches to address new vulnerabilities. These should also be checked. Constant vigilance is required to protect your business.

Any effective cybersecurity procedure includes user education and training. Make certain any employees, licensed or unlicensed, know their data security employment requirements. The requirements should be in your WSPs/P&P documents and part of the firm's supervision duties for designated officials and other supervisory personnel.

Full Checklist

Detect: Anti-Virus Protection and Firewalls
1. The investment adviser firm regularly uses anti-virus software on all devices accessing the firm's network, including mobile phones.
2. The investment adviser understands how the anti-virus software deploys and how to handle alerts.
3. Anti-virus updates are run on a regular and continuous basis.
4. All software is scheduled for automatic updates.
5. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.
6. If the alerts are set up by an outside vendor, there is an ongoing relationship between the vendor and the investment adviser to ensure continuity and updates.
7. A firewall is employed and configured appropriate to the firm's needs.
8. The firm has policies and procedures to address flagged network events.

Examination Questions for "Detect: Anti-Virus Protection and Firewalls"

Detect: Anti-Virus Protection and Firewalls
1. The investment adviser firm regularly uses anti-virus software on all devices accessing the firm's network, including mobile phones.
3. Anti-virus updates are run on a regular and continuous basis.
4. All software is scheduled for automatic updates.
5. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.
7. A firewall is employed and configured appropriate to the firm's needs.

Respond: Responding to a Cyber Event

This Checklist section includes wise business risk management suggestions so you are prepared for a data breach event. While this section has no examination questions, your firm should anticipate new regulatory requirements if and when the current SEC proposed rules are finalized.

Note: Although there are no specific securities regulations, you may be subject to other laws concerning reporting data breaches for your business. These laws include SEC regulations for certain public entities, Utah data breach laws, and other laws in each state where you have clients. In the event of a data breach, you should *seek competent legal counsel* to address all applicable laws.

Full Checklist

Respond: Responding to a Cyber Event
1. The investment adviser has a plan and procedure for immediately notifying authorities in the case of a disaster or security incident.
2. The plans and procedures identify which authorities should be contacted based on the type of incident and who should be responsible for initiating those contacts.
3. The investment adviser has a communications plan, which identifies who will speak to the public/press in the case of an incident and how internal communications will be managed.
4. The communications plan identifies the process for notifying clients.

Examination Question for "Respond: Responding to a Cyber Event"

There are no examination questions for this checklist section.

Recover: Cyber-Insurance

There are no current or proposed regulations requiring the purchase of cyber insurance for RIA firms. The purpose of this examination question is to learn the percentage of Utah state-covered RIA firms that have considered or explored purchasing cyber insurance. Thus, there is no correct or incorrect answer.

Every firm is subject to cybersecurity risk as one of the risks of conducting business with computing, digital communications, digital records collection, and storage activities. It does make sense for firm owners to assess the business risks and determine if any risks are presently covered by current insurance and if the cost of additional insurance protection is worth the expense.

Full Checklist

Recover: Cyber-insurance
1. The investment adviser has considered whether cyber insurance is necessary or appropriate for the firm.
2. The firm has evaluated the coverage in a cybersecurity insurance policy to determine whether it covers breaches, including breaches by foreign cyber intruders, insider breaches (e.g. an employee who steals sensitive data), and breaches as a result of third-party relationships.
3. The cybersecurity insurance policy covers notification (clients and regulators) costs.
4. The investment adviser has evaluated whether the policy includes first-party coverage (e.g., damages associated with theft, data loss, hacking, and denial of service attacks) or third-party coverage (e.g., legal expenses, notification expenses, third-party remediation expenses).
5. The exclusions of the cybersecurity insurance policy are appropriate for the investment adviser's business model.
6. The investment adviser has put into place all safeguards necessary to ensure that the cyber-security policy is not voided through investment adviser employee actions, such as negligent computer security where software patches and updates are not installed in a timely manner.

Examination Question for "Recover: Cyber-Insurance"

Recover: Cyber-insurance
1. The investment adviser has considered whether cyber insurance is necessary or appropriate for the firm. [SURVEY QUESTION]

Recover: Disaster Recovery

In 2003, the SEC issued Release IA-2204 "Compliance Programs of Investment Companies and Investment Advisers".[15] In the rule, the SEC discussed 1) the need for advisers to establish a reasonable process for responding to emergencies, contingencies, and disasters; and 2) an adviser's contingency planning process should be appropriately scaled and reasonable in light of the facts and circumstances surrounding the adviser's business operations, and the commitments it has made to its clients. A cybersecurity event could rise to this level of an "emergency". Firms, in their WSP/P&P documents, should address business outages and create plans to remedy an outage.

Current RIA books and records rules require firms to separately store preserved records to access, view, and print a requested record for a regulatory authority.[16] Hence, there is a need for a process to retrieve backed-up information. These processes need to be memorialized in the firm's WSP/P&P documents.

Full Checklist

Recover: Disaster Recovery
1. The investment adviser has a business continuity plan to implement in the event of a cybersecurity event.
2. The investment adviser has a process for retrieving backed up data and archival copies of information.
3. The investment adviser has written policies and procedures for employees regarding the storage and archival of information.
4. The investment adviser provides training on the recovery process.

Examination Questions for "Recover: Disaster Recovery"

Recover: Disaster Recovery
1. The investment adviser has a business continuity plan to implement in the event of a cybersecurity event.
2. The investment adviser has a process for retrieving backed-up data and archival copies of information.
3. The investment adviser has written policies and procedures for employees regarding the storage and archival of information.

[15] *Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Release No. 2204 (Dec. 17, 2003), SEC.GOV, https://www.sec.gov/rule-release/ia-2204.

[16] *See Appendix D* for the books and records requirements.

Conclusion

This completes the examination instruction guide. Please complete the examination submission form using this link[17] to a Google Form with the examination questions. You will automatically receive a copy of your answers for your records to the email address you enter on the Google Form. Please complete all fields and answer all questions for an error-free submission. If you have trouble with the Google Form submission, contact your assigned Examiner identified in the Exam Cover Letter.

For examination questions that are labeled as "SURVEY QUESTIONS", there is no right or wrong answer. All other exam questions should have a "YES" response. This is because the question involves a current regulatory obligation. For examination questions that require an action on your part to answer "YES" (e.g. an update to firm WSP or P&P documents, employee training, using software features to safeguard Regulation S-P non-public information, etc.), you must complete the action **before** submitting the Examination Submission Form to answer the question accurately.

If you answer "NO" to a current regulatory compliance requirement question, you need to follow up the response with an outline of what you will do to become compliant with the requirement, along with a deadline date for completion. Contact your assigned Examiner to make arrangements to deliver your proposed outline to clear any examination deficiencies.

The Division is providing you with **30 days from the date of your Examination Cover Letter to submit the Examination Submission Form**. However, if you are unable to comply with this deadline, contact the Securities Examiner as soon as possible and before the 30-day deadline expires. The Division will work with you to ensure a timely completion of the examination.

Should you have questions, please contact your assigned Examiner. The Division thanks you in advance for your cooperation with this Special Examination.

[17] If the hyperlink doesn't work, use this link: https://forms.gle/CCDK5F5kFC2CPVFCA.

Appendix

A- Cybersecurity Risk Management Proposed Rule 33-11028 Fact Sheet.
B- Proposed Enhancements to Regulation S-P 34-97141 Fact Sheet.
C- NASAA Cybersecurity Checklist.
D- SEC Books and Records Requirements 17 CFR § 275.204-2.
E- SEC Compliance Procedures and Practices 17 CFR § 275.206(4)-7.
F- Sample Examination Submission Form.

FACT SHEET

Cybersecurity Risk Management

The Commission is proposing new cybersecurity risk management rules and related amendments to certain rules under the Investment Advisers Act of 1940 (the "Advisers Act") and the Investment Company Act of 1940 (the "Investment Company Act"). The proposed rules and amendments would enhance cybersecurity preparedness and improve the resilience of investment advisers and investment companies against cybersecurity threats and attacks by:

- Requiring advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks;
- Having advisers report significant cybersecurity incidents to the Commission on proposed Form ADV-C;
- Enhancing adviser and fund disclosures related to cybersecurity risks and incidents; and
- Requiring advisers and fund to maintain, make, and retain certain cybersecurity-related books and records.

Background

Advisers and funds play an important role in our financial markets and increasingly depend on technology for critical business operations. Advisers and funds are exposed to, and rely on, a broad array of interconnected systems and networks, both directly and through service providers such as custodians, brokers, dealers, pricing services, and other technology vendors. As a result, they face numerous cybersecurity risks and may experience cybersecurity incidents that can cause, or be exacerbated by, critical system or process failures.

The Commission is concerned about the efficacy of adviser and fund practices industry-wide to address cybersecurity risks and incidents, and that less robust cybersecurity practices may not adequately address investor protection concerns. There is also concern about the effectiveness of disclosures to advisory clients and fund shareholders concerning cybersecurity risks and incidents. The Commission's proposed rules and amendments are designed to address concerns about advisers' and funds' cybersecurity preparedness and reduce cybersecurity-related risks to clients and investors; to improve the disclosures clients and investors receive about advisers' and funds' cybersecurity exposures and the cybersecurity incidents that occur at advisers and funds; and to enhance the Commission's ability to assess systemic risks and its oversight of advisers and funds.

Proposed Amendments

Cybersecurity Risk Management Rules

The proposal includes new rule 206(4)-9 under the Advisers Act and new rule 38a-2 under the Investment Company Act (collectively, the "proposed cybersecurity risk management

rules"). The proposed cybersecurity risk management rules would require advisers and funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks. The proposed rules enumerate certain general elements that advisers and funds would be required to address in their cybersecurity policies and procedures. These policies and procedures would help address operational and other risks that could harm advisory clients and fund investors or lead to the unauthorized access to or use of adviser or fund information, including the personal information of their clients or investors.

Reporting of Significant Cybersecurity Incidents

The proposal also includes a reporting requirement under new rule 204-6 that would require advisers to report significant cybersecurity incidents to the Commission, including on behalf of a fund or private fund client. The adviser would have to report by submitting a new Form ADV-C. These confidential reports would bolster the efficiency and effectiveness of the Commission's efforts to protect investors by helping the Commission monitor and evaluate the effects of a cybersecurity incident on an adviser and its clients, as well as assess the potential systemic risks affecting financial markets more broadly.

Disclosure of Cybersecurity Risks and Incidents

Currently, advisers provide disclosures to their prospective and current clients on Form ADV's narrative brochure, or Part 2A, which is publicly available and one of the primary client-facing disclosure documents used by advisers. Form ADV Part 2A contains information about the investment adviser's business practices, fees, risks, conflicts of interest, and disciplinary information. The proposal includes amendments to Form ADV Part 2A to require disclosure of cybersecurity risks and incidents to an adviser's clients and prospective clients.

Like advisers, funds would also be required to provide prospective and current investors with cybersecurity-related disclosures. More specifically, the proposed amendments would require a description of any significant fund cybersecurity incidents that has occurred in the last two fiscal years in funds' registration statements, tagged in a structured data language. The proposal includes amendments to Form N-1A, Form N-2, Form N-3, Form N-4, Form N-6, Form N-8B-2, and Form S-6.

Recordkeeping

The proposal also includes new recordkeeping requirements under the Advisers Act and Investment Company Act. Rule 204-2, the books and records rule, under the Advisers Act sets forth requirements for maintaining, making, and retaining books and records relating to an adviser's investment advisory business. The proposal would amend this rule to require advisers to maintain certain records related to the proposed cybersecurity risk management rules and the occurrence of cybersecurity incidents.

Similarly, proposed rule 38a-2 under the Investment Company Act would require that a fund maintain copies of its cybersecurity policies and procedures and other related records specified under the proposed rule.

Additional Information:

The initial comment period closed on April 11, 2022. The comment period was reopened on March 15, 2023, and will remain open until 60 days after the date of publication of the reopening release in the Federal Register.

FACT SHEET

Proposed Enhancements to Regulation S-P

The Securities and Exchange Commission proposed enhancements to Regulation S-P – the regulation protecting privacy of consumer financial information – to require broker-dealers, investment companies, registered investment advisers, and transfer agents (collectively, "covered institutions) to notify individuals affected by certain types of data breaches that may put them at risk of harm. The proposed amendments would enhance protections of customer information by:

- Requiring covered institutions to adopt written policies and procedures for an incident response program to address unauthorized access to or use of customer information;
- Requiring covered institutions to have written policies and procedures to provide timely notification to affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization; and
- Broadening the scope of information covered by Regulation S-P's requirements.

Why This Matters

In 2000, the Commission adopted Regulation S-P, which: (1) broadly requires broker-dealers, investment companies, and registered investment advisers to adopt written policies and procedures to safeguard customer records and information (the "safeguards rule" – Rule 248.30(a)); (2) requires proper disposal of consumer report information in a manner that protects against unauthorized access to or use of such information (the "disposal rule" – Rule 248.30(b)); and (3) implemented privacy policy notice and opt out provisions required by Congress.

Since Regulation S-P's adoption, evolution in the technological landscape has made it easier for firms to obtain, share, and maintain individuals' personal information, which has exacerbated the risk of unauthorized access to or use of customer information. The protections afforded to a customer of a covered institution in one state may differ substantially from the protections afforded to a customer of the same type of institution in another state.

How This Rule Would Apply

The proposal would establish a Federal minimum standard for covered institutions to provide data breach notifications to affected individuals.

Incident Response Program

To help protect against harms that may result from a security incident involving customer information, the proposed amendments would require covered institutions to adopt an incident response program as part of their written policies and procedures under the safeguards rule. The proposal would require an incident response program to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, include procedures to assess the nature and scope of any such incident, and contain and control such incidents. The proposal would also apply certain requirements related to incident response to covered institutions' relationships with third party service providers.

Customer Notification Requirement

The proposed amendments would require covered institutions to notify affected individuals whose sensitive customer information was or is reasonably likely to have been accessed or used without authorization. The proposal would require a covered institution to provide the notice as soon as practicable, but not later than 30 days after a covered institution becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. A covered institution would not need to provide the notification if the covered institution determines that the sensitive customer information was not actually and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience.

The proposed enhancements to Regulation S-P would also:

- Expand the safeguards and disposal rules to cover "customer information," a new defined term referring to a record containing "nonpublic personal information," a term already in use for other components of Regulation S-P, about a customer of a financial institution. The proposed amendments would therefore apply both rules to both nonpublic personal information that a covered institution collects about its own customers and nonpublic personal information it receives from a third party financial institution about customers of that financial institution;
- Require covered institutions to make and maintain written records documenting compliance with the requirements of the safeguards rule and disposal rule;
- Conform Regulation S-P's annual privacy notice delivery provisions to the terms of an exception added by the 2015 Fixing America's Surface Transportation Act, which would provide that covered institutions are not required to deliver an annual privacy notice if certain conditions are satisfied; and
- Extend the safeguards rule to transfer agents registered with the Commission or another appropriate regulatory agency. In addition, the proposed amendments would extend the disposal rule from covering only transfer agents registered with the Commission to also transfer agents registered with another appropriate regulatory agency.

Additional Information:

The public comment period will remain open until 60 days after the date of publication of the proposing release in the Federal Register.

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION
Cybersecurity Checklist for Investment Advisers

Issued: 2017 Modified 2023

Identify Protect Detect Respond Recover

Identify: Risk Assessments & Management	YES	NO	N/A
1. Risk assessments are conducted frequently (e.g. annually, quarterly).			
2. Cybersecurity is included in the risk assessment.			
3. The risk assessment includes a review of the data collected or created, where the data is stored, and if the data is encrypted.			
4. Internal "insider" risk (e.g. disgruntled employees) and external risks are included in the risk assessment.			
5. The risk assessment includes relationships with third parties.			
6. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices (e.g. frequent password changes, locking of devices, reporting of lost or stolen devices, etc.).			
7. Primary and secondary person(s) are assigned as the central point of contact in the event of a cybersecurity incident.			
8. Specific roles and responsibilities are tasked to the primary and secondary person(s) regarding a cybersecurity incident.			
9. The firm has an inventory of all hardware and software.			
Protect: Use of Electronic Mail	YES	NO	N/A
1. Identifiable information of a client is transmitted via email.			
2. Authentication practices for access to email on all devices (computer and mobile devices) is required.			
3. Passwords for access to email are changed frequently (e.g. monthly, quarterly).			
4. Policies and procedures detail how to authenticate client instructions received via email.			
5. Email communications are secured. (If the response is no, proceed to the next question.)			
6. Employees and clients are aware that email communication is not secured.			
Protect: Devices	YES	NO	N/A
1. Device access (physical and digital) is permitted for authorized users, including personnel and clients.			
2. Device access is routinely audited and updated appropriately.			
3. Devices are routinely backed up and underlying data is stored in a separate location (i.e. on an external drive, in the cloud, etc.)			
4. Backups are routinely tested.			
5. The investment adviser has written policies and procedures regarding destruction of electronic data and physical documents.			
6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures.			
Protect: Use of Cloud Services	YES	NO	N/A
1. Due diligence has been conducted on the cloud service provider prior to signing an agreement or contract.			
2. As part of the due diligence, the investment adviser has evaluated whether the cloud service provider has safeguards against breaches and a documented process in the event of breaches.			

Protect: Use of Cloud Services (cont.)	YES	NO	N/A
3. The investment adviser has a business relationship with the cloud service provider and has the contact information for that entity.			
4. The investment adviser is aware of the assignability terms of the contract.			
5. The investment adviser understands how the firm's data is segregated from other entities' data within the cloud service.			
6. The investment adviser is familiar with the restoration procedures in the event of a breach or loss of data stored through the cloud service.			
7. The investment adviser has written policies and procedures in the event that the cloud service provider is purchased, closed, or otherwise unable to be accessed.			
8. The investment adviser solely relies on free cloud storage.			
9. The investment adviser has a back-up of all records off-site.			
10. Data containing sensitive or personally identifiable information is stored through a cloud service.			
11. Data containing sensitive or personally identifiable information, which is stored through a cloud service, is encrypted.			
12. The investment adviser has written policies and procedures related to the use of mobile devices by staff who access data in the cloud.			
13. The cloud service provider (or its staff) may access and/or view the investment adviser's data stored in the cloud.			
14. The investment adviser allows remote access to its network (e.g. through use of VPN).			
15. The VPN access of employees is monitored.			
16. The investment adviser has written policies and procedures related to the termination of VPN access when an employee resigns or is terminated.			
Protect: Use of Firm Websites	YES	NO	N/A
1. The investment adviser relies on a parent or affiliated company for the construction and maintenance of the website.			
2. The investment adviser relies on internal personnel for the construction and maintenance of the website.			
3. The investment adviser relies on a third-party vendor for the construction and maintenance of the website.			
4. If the investment adviser relies on a third party for website maintenance, there is an agreement with the third party regarding the services and the confidentiality of information.			
5. The investment adviser can directly make changes to the website.			
6. The investment adviser can directly access the domain renewal information and the security certificate information.			
7. The firm's website is used to access client information.			
8. SSL or other encryption is used when accessing client information on the firm's website.			
9. The firm's website includes a client portal.			
10. SSL or other encryption is used when accessing a client portal.			
11. When accessing the client portal, user authentication credentials (i.e., user name and password) are encrypted.			
12. Additional authentication credentials (i.e., challenge questions, etc.) are required when accessing the client portal from an unfamiliar network or computer.			
13. The investment adviser has written policies and procedures related to a denial of service issue.			
Protect: Custodians & Other Third-Party Vendors	YES	NO	N/A
1. The investment adviser's due diligence on third parties includes cybersecurity as a component.			

Protect: Custodians & Other Third-Party Vendors (cont.)	YES	NO	N/A
2. The investment adviser has requested vendors to complete a cybersecurity questionnaire with a focus on issues of liability sharing and whether vendors have policies and procedures based on industry standards.			
3. The investment adviser understands that the vendor has IT staff or outsources some functions.			
4. The investment adviser has obtained a written attestation from the vendor that it uses software to ensure customer data is protected.			
5. The investment adviser has inquired whether a vendor performs a cybersecurity risk assessment or audit on a regular basis.			
6. The cyber-security terms of the agreement with an outside vendor is not voided because of the actions of an employee of the investment adviser.			
7. Confidentiality agreements are signed by the investment adviser and third-party vendors.			
8. The investment adviser has been provided enough information to assess the cybersecurity practices of any third-party vendors.			
9. [Relevant to custodians only] The investment adviser has discussed with the custodian matters regarding the impersonation of clients and authentication of client orders.			
Protect: Encryption	YES	NO	N/A
1. The investment adviser routinely consults with an IT professional knowledgeable in cybersecurity.			
2. The investment adviser has written policies and procedures in place to categorize data as either confidential or non-confidential.			
3. The investment adviser has written policies and procedures in place to address data security and/or encryption requirements.			
4. The investment adviser has written policies and procedures in place to address the physical security of confidential data and systems containing confidential data (i.e., servers, laptops, tablets, removable media, etc.).			
5. The investment adviser utilizes encryption on all data systems that contain (or access) confidential information.			
6. The identities and credentials of authorized users are monitored.			
Detect: Anti-Virus Protection and Firewalls	YES	NO	N/A
1. The investment adviser firm regularly uses anti-virus software on all devices accessing the firm's network, including mobile phones.			
2. The investment adviser understands how the anti-virus software deploys and how to handle alerts.			
3. Anti-virus updates are run on a regular and continuous basis.			
4. All software is scheduled for automatic updates.			
5. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.			
6. If the alerts are set up by an outside vendor, there is an ongoing relationship between the vendor and the investment adviser to ensure continuity and updates.			
7. A firewall is employed and configured appropriate to the firm's needs.			
8. The firm has policies and procedures to address flagged network events.			
Respond: Responding to a Cyber Event	YES	NO	N/A
1. The investment adviser has a plan and procedure for immediately notifying authorities in the case of a disaster or security incident.			

Respond: Responding to a Cyber Event (cont.)	YES	NO	N/A
2. The plans and procedures identify which authorities should be contacted based on the type of incident and who should be responsible for initiating those contacts.			
3. The investment adviser has a communications plan, which identifies who will speak to the public/press in the case of an incident and how internal communications will be managed.			
4. The communications plan identifies the process for notifying clients.			
Recover: Cyber-insurance	YES	NO	N/A
1. The investment adviser has considered whether cyber-insurance is necessary or appropriate for the firm.			
2. The firm has evaluated the coverage in a cybersecurity insurance policy to determine whether it covers breaches, including; breaches by foreign cyber intruders; insider breaches (e.g. an employee who steals sensitive data); and breaches as a result of third-party relationships.			
3. The cybersecurity insurance policy covers notification (clients and regulators) costs.			
4. The investment adviser has evaluated whether the policy includes first-party coverage (e.g., damages associated with theft, data loss, hacking, and denial of service attacks) or third-party coverage (e.g., legal expenses, notification expenses, third-party remediation expenses).			
5. The exclusions of the cybersecurity insurance policy are appropriate for the investment adviser's business model.			
6. The investment adviser has put into place all safeguards necessary to ensure that the cyber-security policy is not voided through investment adviser employee actions, such as negligent computer security where software patches and updates are not installed in a timely manner.			
Recover: Disaster Recovery	YES	NO	N/A
1. The investment adviser has a business continuity plan to implement in the event of a cybersecurity event.			
2. The investment adviser has a process for retrieving backed-up data and archival copies of information.			
3. The investment adviser has written policies and procedures for employees regarding the storage and archival of information.			
4. The investment adviser provides training on the recovery process.			

INFORMATION GPO

adviser provides continuous and regular supervisory or management services as reported on the investment adviser's Form ADV (17 CFR 279.1).

(e) *State securities authority.* "State securities authority" means the securities commissioner or commission (or any agency, office or officer performing like functions) of any State.

[62 FR 28134, May 22, 1997, as amended at 63 FR 39715, July 24, 1998; 69 FR 72088, Dec. 10, 2004; 76 FR 43012, July 19, 2011]

§§ 275.203A–4—275.203A–6 [Reserved]

§ 275.204–1 Amendments to Form ADV.

(a) *When amendment is required.* You must amend your Form ADV (17 CFR 279.1):

(1) Parts 1 and 2:

(i) At least annually, within 90 days of the end of your fiscal year; and

(ii) More frequently, if required by the instructions to Form ADV.

(2) Part 3 at the frequency required by the instructions to Form ADV.

(b) *Electronic filing of amendments.* (1) Subject to paragraph (c) of this section, you must file all amendments to Part 1A, Part 2A, and Part 3 of Form ADV electronically with the IARD, unless you have received a continuing hardship exemption under § 275.203–3. You are not required to file with the Commission amendments to brochure supplements required by Part 2B of Form ADV.

(2) If you have received a continuing hardship exemption under § 275.203–3, you must, when you are required to amend your Form ADV, file a completed Part 1A, Part 2A and Part 3 of Form ADV on paper with the SEC by mailing it to FINRA.

(c) *Filing fees.* You must pay FINRA (the operator of the IARD) an initial filing fee when you first electronically file Part 1A of Form ADV. After you pay the initial filing fee, you must pay an annual filing fee each time you file your annual updating amendment. No portion of either fee is refundable. The Commission has approved the filing fees. Your amended Form ADV will not be accepted by FINRA, and thus will not be considered filed with the Commission, until you have paid the filing fee.

(d) *Amendments to Form ADV are reports.* Each amendment required to be filed under this section is a "report" within the meaning of sections 204 and 207 of the Act (15 U.S.C. 80b–4 and 80b–7).

(e) *Transition to Filing Form CRS.* If you are registered with the Commission or have an application for registration pending with the Commission prior to June 30, 2020, you must amend your Form ADV by electronically filing with IARD your initial Form CRS that satisfies the requirements of Part 3 of Form ADV (as amended effective September 30, 2019) beginning on May 1, 2020 and by no later than June 30, 2020.

NOTE 1 TO PARAGRAPHS (e): This note applies to paragraphs (a), (b), and (e) of this section. Information on how to file with the IARD is available on our website at *http://www.sec.gov/iard.* For the annual updating amendment: Summaries of material changes that are not included in the adviser's brochure must be filed with the Commission as an exhibit to Part 2A in the same electronic file; and if you are not required to prepare a brochure, a summary of material changes, an annual updating amendment to your brochure, or Form CRS you are not required to file them with the Commission. See the instructions for Part 2A and Part 3 of Form ADV.

[65 FR 57450, Sept. 22, 2000; 65 FR 81738, Dec. 27, 2000, as amended at 68 FR 42248, July 17, 2003; 73 FR 4694, Jan. 28, 2008; 75 FR 49267, Aug. 12, 2010; 76 FR 43013, July 19, 2011; 81 FR 60458, Sept. 1, 2016; 84 FR 33630, July 12, 2019]

§ 275.204–2 Books and records to be maintained by investment advisers.

(a) Every investment adviser registered or required to be registered under section 203 of the Act (15 U.S.C. 80b–3) shall make and keep true, accurate and current the following books and records relating to its investment advisory business;

(1) A journal or journals, including cash receipts and disbursements, records, and any other records of original entry forming the basis of entries in any ledger.

(2) General and auxiliary ledgers (or other comparable records) reflecting asset, liability, reserve, capital, income and expense accounts.

(3) A memorandum of each order given by the investment adviser for the purchase or sale of any security, of any instruction received by the investment

adviser concerning the purchase, sale, receipt or delivery of a particular security, and of any modification or cancellation of any such order or instruction. Such memoranda shall show the terms and conditions of the order, instruction, modification or cancellation; shall identify the person connected with the investment adviser who recommended the transaction to the client and the person who placed such order; and shall show the account for which entered, the date of entry, and the bank, broker or dealer by or through whom executed where appropriate. Orders entered pursuant to the exercise of discretionary power shall be so designated.

(4) All check books, bank statements, cancelled checks and cash reconciliations of the investment adviser.

(5) All bills or statements (or copies thereof), paid or unpaid, relating to the business of the investment adviser as such.

(6) All trial balances, financial statements, and internal audit working papers relating to the business of such investment adviser.

(7) Originals of all written communications received and copies of all written communications sent by such investment adviser relating to:

(i) Any recommendation made or proposed to be made and any advice given or proposed to be given;

(ii) Any receipt, disbursement or delivery of funds or securities;

(iii) The placing or execution of any order to purchase or sell any security;

(iv) Predecessor performance (as defined in §275.206(4)–1(e)(12) of this chapter) and the performance or rate of return of any or all managed accounts, portfolios (as defined in §275.206(4)–1(e)(11) of this chapter), or securities recommendations; Provided, however:

(A) That the investment adviser shall not be required to keep any unsolicited market letters and other similar communications of general public distribution not prepared by or for the investment adviser; and

(B) That if the investment adviser sends any notice, circular, or other advertisement (as defined in §275.206(4)–1(e)(1) of this chapter) offering any report, analysis, publication or other investment advisory service to more than ten persons, the investment adviser shall not be required to keep a record of the names and addresses of the persons to whom it was sent; except that if such notice, circular, or advertisement is distributed to persons named on any list, the investment adviser shall retain with the copy of such notice, circular, or advertisement a memorandum describing the list and the source thereof.

(8) A list or other record of all accounts in which the investment adviser is vested with any discretionary power with respect to the funds, securities or transactions of any client.

(9) All powers of attorney and other evidences of the granting of any discretionary authority by any client to the investment adviser, or copies thereof.

(10) All written agreements (or copies thereof) entered into by the investment adviser with any client or otherwise relating to the business of such investment adviser as such.

(11)(i) A copy of each

(A) Advertisement (as defined in §275.206(4)–1(e)(1) of this chapter) that the investment adviser disseminates, directly or indirectly, except:

(*1*) For oral advertisements, the adviser may instead retain a copy of any written or recorded materials used by the adviser in connection with the oral advertisement; and

(*2*) For compensated oral testimonials and endorsements (as defined in §275.206(4)–1(e)(17) and (5) of this chapter), the adviser may instead make and keep a record of the disclosures provided to clients or investors pursuant to §275.206(4)–1(b)(1) of this chapter; and

(B) Notice, circular, newspaper article, investment letter, bulletin, or other communication that the investment adviser disseminates, directly or indirectly, to ten or more persons (other than persons associated with such investment adviser); and

(C) If such notice, circular, advertisement, newspaper article, investment letter, bulletin, or other communication recommends the purchase or sale of a specific security and does not state the reasons for such recommendation, a memorandum of the investment adviser indicating the reasons therefor; and

(ii) A copy of any questionnaire or survey used in the preparation of a third-party rating included or appearing in any advertisement in the event the adviser obtains a copy of the questionnaire or survey.

(12)(i) A copy of the investment adviser's code of ethics adopted and implemented pursuant to § 275.204A–1 that is in effect, or at any time within the past five years was in effect;

(ii) A record of any violation of the code of ethics, and of any action taken as a result of the violation; and

(iii) A record of all written acknowledgments as required by § 275.204A–1(a)(5) for each person who is currently, or within the past five years was, a supervised person of the investment adviser.

(13)(i) A record of each report made by an access person as required by § 275.204A–1(b), including any information provided under paragraph (b)(3)(iii) of that section in lieu of such reports;

(ii) A record of the names of persons who are currently, or within the past five years were, access persons of the investment adviser; and

(iii) A record of any decision, and the reasons supporting the decision, to approve the acquisition of securities by access persons under § 275.204A–1(c), for at least five years after the end of the fiscal year in which the approval is granted.

(14)(i) A copy of each brochure, brochure supplement and Form CRS, and each amendment or revision to the brochure, brochure supplement and Form CRS, that satisfies the requirements of Part 2 or Part 3 of Form ADV, as applicable [17 CFR 279.1]; any summary of material changes that satisfies the requirements of Part 2 of Form ADV but is not contained in the brochure; and a record of the dates that each brochure, brochure supplement and Form CRS, each amendment or revision thereto, and each summary of material changes not contained in a brochure given to any client or to any prospective client who subsequently becomes a client.

(ii) Documentation describing the method used to compute managed assets for purposes of Item 4.E of Part 2A of Form ADV, if the method differs from the method used to compute regulatory assets under management in Item 5.F of Part 1A of Form ADV.

(iii) A memorandum describing any legal or disciplinary event listed in Item 9 of Part 2A or Item 3 of Part 2B (Disciplinary Information) and presumed to be material, if the event involved the investment adviser or any of its supervised persons and is not disclosed in the brochure or brochure supplement described in paragraph (a)(14)(i) of this section. The memorandum must explain the investment adviser's determination that the presumption of materiality is overcome, and must discuss the factors described in Item 9 of Part 2A of Form ADV or Item 3 of Part 2B of Form ADV.

(15)(i) If not included in the advertisement, a record of the disclosures provided to clients or investors pursuant to § 275.206(4)–1(b)(1)(ii) and (iii) of this chapter;

(ii) Documentation substantiating the adviser's reasonable basis for believing that a testimonial or endorsement (as defined in § 275.206(4)–1(e)(17) and (5) of this chapter) complies with § 275.206(4)–1 and that the third-party rating (as defined in § 275.206(4)–1(e)(18) of this chapter) complies with § 275.206(4)–1(c)(1) of this chapter.

(iii) A record of the names of all persons who are an investment adviser's partners, officers, directors, or employees, or a person that controls, is controlled by, or is under common control with the investment adviser, or is a partner, officer, director or employee of such a person pursuant to § 275.206(4)–1(b)(4)(ii) of this chapter.

(16) All accounts, books, internal working papers, and any other records or documents that are necessary to form the basis for or demonstrate the calculation of any performance or rate of return of any or all managed accounts, portfolios (as defined in § 275.206(4)–1(e)(11) of this chapter), or securities recommendations presented in any notice, circular, advertisement (as defined in § 275.206(4)–1(e)(1) of this chapter), newspaper article, investment letter, bulletin, or other communication that the investment adviser disseminates, directly or indirectly, to

any person (other than persons associated with such investment adviser), including copies of all information provided or offered pursuant to § 275.206(4)–1(d)(6) of this chapter; provided, however, that, with respect to the performance of managed accounts, the retention of all account statements, if they reflect all debits, credits, and other transactions in a client's or investor's account for the period of the statement, and all worksheets necessary to demonstrate the calculation of the performance or rate of return of all managed accounts shall be deemed to satisfy the requirements of this paragraph.

(17)(i) A copy of the investment adviser's policies and procedures formulated pursuant to § 275.206(4)–7(a) of this chapter that are in effect, or at any time within the past five years were in effect;

(ii) Any records documenting the investment adviser's annual review of those policies and procedures conducted pursuant to § 275.206(4)–7(b) of this chapter;

(iii) A copy of any internal control report obtained or received pursuant to § 275.206(4)–2(a)(6)(ii).

(18)(i) Books and records that pertain to § 275.206(4)–5 containing a list or other record of:

(A) The names, titles and business and residence addresses of all covered associates of the investment adviser;

(B) All government entities to which the investment adviser provides or has provided investment advisory services, or which are or were investors in any covered investment pool to which the investment adviser provides or has provided investment advisory services, as applicable, in the past five years, but not prior to September 13, 2010;

(C) All direct or indirect contributions made by the investment adviser or any of its covered associates to an official of a government entity, or direct or indirect payments to a political party of a State or political subdivision thereof, or to a political action committee; and

(D) The name and business address of each regulated person to whom the investment adviser provides or agrees to provide, directly or indirectly, payment to solicit a government entity for investment advisory services on its behalf, in accordance with § 275.206(4)–5(a)(2).

(ii) Records relating to the contributions and payments referred to in paragraph (a)(18)(i)(C) of this section must be listed in chronological order and indicate:

(A) The name and title of each contributor;

(B) The name and title (including any city/county/State or other political subdivision) of each recipient of a contribution or payment;

(C) The amount and date of each contribution or payment; and

(D) Whether any such contribution was the subject of the exception for certain returned contributions pursuant to § 275.206(4)–5(b)(2).

(iii) An investment adviser is only required to make and keep current the records referred to in paragraphs (a)(18)(i)(A) and (C) of this section if it provides investment advisory services to a government entity or a government entity is an investor in any covered investment pool to which the investment adviser provides investment advisory services.

(iv) For purposes of this section, the terms "contribution," "covered associate," "covered investment pool," "government entity," "official," "payment," "regulated person," and "solicit" have the same meanings as set forth in § 275.206(4)–5.

(19) A record of who the "intended audience" is pursuant to § 275.206(4)–1(d)(6) and(e)(10)(ii)(B) of this chapter.

(b) If an investment adviser subject to paragraph (a) of this section has custody or possession of securities or funds of any client, the records required to be made and kept under paragraph (a) of this section shall include:

(1) A journal or other record showing all purchases, sales, receipts and deliveries of securities (including certificate numbers) for such accounts and all other debits and credits to such accounts.

(2) A separate ledger account for each such client showing all purchases, sales, receipts and deliveries of securities, the date and price of each purchase and sale, and all debits and credits.

(3) Copies of confirmations of all transactions effected by or for the account of any such client.

(4) A record for each security in which any such client has a position, which record shall show the name of each such client having any interest in such security, the amount or interest of each such client, and the location of each such security.

(5) A memorandum describing the basis upon which you have determined that the presumption that any related person is not operationally independent under § 275.206(4)–2(d)(5) has been overcome.

(c)(1) Every investment adviser subject to paragraph (a) of this section who renders any investment supervisory or management service to any client shall, with respect to the portfolio being supervised or managed and to the extent that the information is reasonably available to or obtainable by the investment adviser, make and keep true, accurate and current:

(i) Records showing separately for each such client the securities purchased and sold, and the date, amount and price of each such purchase and sale.

(ii) For each security in which any such client has a current position, information from which the investment adviser can promptly furnish the name of each such client, and the current amount or interest of such client.

(2) Every investment adviser subject to paragraph (a) of this section that exercises voting authority with respect to client securities shall, with respect to those clients, make and retain the following:

(i) Copies of all policies and procedures required by § 275.206(4)–6.

(ii) A copy of each proxy statement that the investment adviser receives regarding client securities. An investment adviser may satisfy this requirement by relying on a third party to make and retain, on the investment adviser's behalf, a copy of a proxy statement (provided that the adviser has obtained an undertaking from the third party to provide a copy of the proxy statement promptly upon request) or may rely on obtaining a copy of a proxy statement from the Commission's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.

(iii) A record of each vote cast by the investment adviser on behalf of a client. An investment adviser may satisfy this requirement by relying on a third party to make and retain, on the investment adviser's behalf, a record of the vote cast (provided that the adviser has obtained an undertaking from the third party to provide a copy of the record promptly upon request).

(iv) A copy of any document created by the adviser that was material to making a decision how to vote proxies on behalf of a client or that memorializes the basis for that decision.

(v) A copy of each written client request for information on how the adviser voted proxies on behalf of the client, and a copy of any written response by the investment adviser to any (written or oral) client request for information on how the adviser voted proxies on behalf of the requesting client.

(d) Any books or records required by this section may be maintained by the investment adviser in such manner that the identity of any client to whom such investment adviser renders investment supervisory services is indicated by numerical or alphabetical code or some similar designation.

(e)(1) All books and records required to be made under the provisions of paragraphs (a) to (c)(1)(i), inclusive, and (c)(2) of this section (except for books and records required to be made under the provisions of paragraphs (a)(11), (a)(12)(i), (a)(12)(iii), (a)(13)(ii), (a)(13)(iii), (a)(16), and (a)(17)(i) of this section), shall be maintained and preserved in an easily accessible place for a period of not less than five years from the end of the fiscal year during which the last entry was made on such record, the first two years in an appropriate office of the investment adviser.

(2) Partnership articles and any amendments thereto, articles of incorporation, charters, minute books, and stock certificate books of the investment adviser and of any predecessor, shall be maintained in the principal office of the investment adviser and preserved until at least three years after termination of the enterprise.

(3)(i) Books and records required to be made under the provisions of paragraphs (a)(11) and (a)(16) of this rule shall be maintained and preserved in an easily accessible place for a period of not less than five years, the first two years in an appropriate office of the investment adviser, from the end of the fiscal year during which the investment adviser last published or otherwise disseminated, directly or indirectly, the notice, circular, advertisement, newspaper article, investment letter, bulletin or other communication.

(ii) *Transition rule.* If you are an investment adviser that was, prior to July 21, 2011, exempt from registration under section 203(b)(3) of the Act (15 U.S.C. 80b–3(b)(3)), as in effect on July 20, 2011, paragraph (e)(3)(i) of this section does not require you to maintain or preserve books and records that would otherwise be required to be maintained or preserved under the provisions of paragraph (a)(16) of this section to the extent those books and records pertain to the performance or rate of return of such private fund (as defined in section 202(a)(29) of the Act (15 U.S.C. 80b–2(a)(29)), or other account you advise for any period ended prior to your registration, provided that you continue to preserve any books and records in your possession that pertain to the performance or rate of return of such private fund or other account for such period.

(f) An investment adviser subject to paragraph (a) of this section, before ceasing to conduct or discontinuing business as an investment adviser shall arrange for and be responsible for the preservation of the books and records required to be maintained and preserved under this section for the remainder of the period specified in this section, and shall notify the Commission in writing, at its principal office, Washington, D.C. 20549, of the exact address where such books and records will be maintained during such period.

(g) *Micrographic and electronic storage permitted*—(1) *General.* The records required to be maintained and preserved pursuant to this part may be maintained and preserved for the required time by an investment adviser on:

(i) Micrographic media, including microfilm, microfiche, or any similar medium; or

(ii) Electronic storage media, including any digital storage medium or system that meets the terms of this section.

(2) *General requirements.* The investment adviser must:

(i) Arrange and index the records in a way that permits easy location, access, and retrieval of any particular record;

(ii) Provide promptly any of the following that the Commission (by its examiners or other representatives) may request:

(A) A legible, true, and complete copy of the record in the medium and format in which it is stored;

(B) A legible, true, and complete printout of the record; and

(C) Means to access, view, and print the records; and

(iii) Separately store, for the time required for preservation of the original record, a duplicate copy of the record on any medium allowed by this section.

(3) *Special requirements for electronic storage media.* In the case of records on electronic storage media, the investment adviser must establish and maintain procedures:

(i) To maintain and preserve the records, so as to reasonably safeguard them from loss, alteration, or destruction;

(ii) To limit access to the records to properly authorized personnel and the Commission (including its examiners and other representatives); and

(iii) To reasonably ensure that any reproduction of a non-electronic original record on electronic storage media is complete, true, and legible when retrieved.

(h)(1) Any book or other record made, kept, maintained and preserved in compliance with §§ 240.17a–3 and 240.17a–4 of this chapter under the Securities Exchange Act of 1934, or with rules adopted by the Municipal Securities Rulemaking Board, which is substantially the same as the book or other record required to be made, kept, maintained and preserved under this section, shall be deemed to be made, kept, maintained and preserved in compliance with this section.

(2) A record made and kept pursuant to any provision of paragraph (a) of this section, which contains all the information required under any other provision of paragraph (a) of this section, need not be maintained in duplicate in order to meet the requirements of the other provision of paragraph (a) of this section.

(i) As used in this section the term "discretionary power" shall not include discretion as to the price at which or the time when a transaction is or is to be effected, if, before the order is given by the investment adviser, the client has directed or approved the purchase or sale of a definite amount of the particular security.

(j)(1) Except as provided in paragraph (j)(3) of this section, each non-resident investment adviser registered or applying for registration pursuant to section 203 of the Act shall keep, maintain and preserve, at a place within the United States designated in a notice from him as provided in paragraph (j)(2) of this section true, correct, complete and current copies of books and records which he is required to make, keep current, maintain or preserve pursuant to any provisions of any rule or regulation of the Commission adopted under the Act.

(2) Except as provided in paragraph (j)(3) of this section, each nonresident investment adviser subject to this paragraph (j) shall furnish to the Commission a written notice specifying the address of the place within the United States where the copies of the books and records required to be kept and preserved by him pursuant to paragraph (j)(1) of this section are located. Each non-resident investment adviser registered or applying for registration when this paragraph becomes effective shall file such notice within 30 days after such rule becomes effective. Each non-resident investment adviser who files an application for registration after this paragraph becomes effective shall file such notice with such application for registration.

(3) Notwithstanding the provisions of paragraphs (j)(1) and (2) of this section, a non-resident investment adviser need not keep or preserve within the United States copies of the books and records referred to in said paragraphs (j)(1) and (2), if:

(i) Such non-resident investment adviser files with the Commission, at the time or within the period provided by paragraph (j)(2) of this section, a written undertaking, in form acceptable to the Commission and signed by a duly authorized person, to furnish to the Commission, upon demand, at its principal office in Washington, DC, or at any Regional Office of the Commission designated in such demand, true, correct, complete and current copies of any or all of the books and records which he is required to make, keep current, maintain or preserve pursuant to any provision of any rule or regulation of the Commission adopted under the Act, or any part of such books and records which may be specified in such demand. Such undertaking shall be in substantially the following form:

> The undersigned hereby undertakes to furnish at its own expense to the Securities and Exchange Commission at its principal office in Washington, DC or at any Regional Office of said Commission specified in a demand for copies of books and records made by or on behalf of said Commission, true, correct, complete and current copies of any or all, or any part, of the books and records which the undersigned is required to make, keep current or preserve pursuant to any provision of any rule or regulation of the Securities and Exchange Commission under the Investment Advisers Act of 1940. This undertaking shall be suspended during any period when the undersigned is making, keeping current, and preserving copies of all of said books and records at a place within the United States in compliance with Rule 204-2(j) under the Investment Advisers Act of 1940. This undertaking shall be binding upon the undersigned and the heirs, successors and assigns of the undersigned, and the written irrevocable consents and powers of attorney of the undersigned, its general partners and managing agents filed with the Securities and Exchange Commission shall extend to and cover any action to enforce same.

and

(ii) Such non-resident investment adviser furnishes to the Commission, at his own expense 14 days after written demand therefor forwarded to him by registered mail at his last address of record filed with the Commission and signed by the Secretary of the Commission or such person as the Commission may authorize to act in its behalf, true, correct, complete and current copies of any or all books and records

which such investment adviser is required to make, keep current or preserve pursuant to any provision of any rule or regulation of the Commission adopted under the Act, or any part of such books and records which may be specified in said written demand. Such copies shall be furnished to the Commission at its principal office in Washington, DC, or at any Regional Office of the Commission which may be specified in said written demand.

(4) For purposes of this rule the term *non-resident investment adviser* shall have the meaning set out in §275.0–2(d)(3) under the Act.

(k) Every investment adviser that registers under section 203 of the Act (15 U.S.C. 80b–3) after July 8, 1997 shall be required to preserve in accordance with this section the books and records the investment adviser had been required to maintain by the State in which the investment adviser had its principal office and place of business prior to registering with the Commission.

[26 FR 5002, June 6, 1961]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting §275.204–2, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at *www.govinfo.gov*.

§275.204–3 Delivery of brochures and brochure supplements.

(a) *General requirements.* If you are registered under the Act as an investment adviser, you must deliver a brochure and one or more brochure supplements to each client or prospective client that contains all information required by Part 2 of Form ADV [17 CFR 279.1].

(b) *Delivery requirements.* Subject to paragraph (g), you (or a supervised person acting on your behalf) must:

(1) Deliver to a client or prospective client your current brochure before or at the time you enter into an investment advisory contract with that client.

(2) Deliver to each client, annually within 120 days after the end of your fiscal year and without charge, if there are material changes in your brochure since your last annual updating amendment:

(i) A current brochure, or

(ii) The summary of material changes to the brochure as required by Item 2 of Form ADV, Part 2A that offers to provide your current brochure without charge, accompanied by the Web site address (if available) and an e-mail address (if available) and telephone number by which a client may obtain the current brochure from you, and the Web site address for obtaining information about you through the Investment Adviser Public Disclosure (IAPD) system.

(3) Deliver to each client or prospective client a current brochure supplement for a supervised person before or at the time that supervised person begins to provide advisory services to the client; provided, however, that if investment advice for a client is provided by a team comprised of more than five supervised persons, a current brochure supplement need only be delivered to that client for the five supervised persons with the most significant responsibility for the day-to-day advice provided to that client. For purposes of this section, a supervised person will provide advisory services to a client if that supervised person will:

(i) Formulate investment advice for the client and have direct client contact; or

(ii) Make discretionary investment decisions for the client, even if the supervised person will have no direct client contact.

(4) Deliver the following to each client promptly after you create an amended brochure or brochure supplement, as applicable, if the amendment adds disclosure of an event, or materially revises information already disclosed about an event, in response to Item 9 of Part 2A of Form ADV or Item 3 of Part 2B of Form ADV (Disciplinary Information), respectively, (i) the amended brochure or brochure supplement, as applicable, along with a statement describing the material facts relating to the change in disciplinary information, or (ii) a statement describing the material facts relating to the change in disciplinary information.

(c) *Exceptions to delivery requirement.* (1) You are not required to deliver a brochure to a client:

recommendations for the proposed information collection should be sent within 30 days of publication of this notice to (i) *MBX.OMB.OIRA.SEC_desk_officer@omb.eop.gov* and (ii) David Bottom, Director/Chief Information Officer, Securities and Exchange Commission, c/o John Pezzullo, 100 F Street NE, Washington, DC 20549, or by sending an email to: *PRA_Mailbox@sec.gov.*

Dated: January 14, 2022.

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2022–01058 Filed 1–19–22; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

[SEC File No. 270–523, OMB Control No. 3235–0585]

Submission for OMB Review; Comment Request; Extension: Rule 206(4)–7

Upon Written Request, Copies Available From: Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington, DC 20549–2736

Notice is hereby given that, pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission (the "Commission") has submitted to the Office of Management and Budget ("OMB") a request for extension of the previously approved collection of information discussed below.

The title for the collection of information is "Investment Advisers Act rule 206(4)–7, 17 CFR Sec. 275.206(4)–7, Compliance procedures and practices." This collection of information is found at 17 CFR 275.206(4)–7, and is mandatory. Rule 206(4)–7 under the Investment Advisers Act of 1940 ("Advisers Act") requires each investment adviser registered with the Commission to (1) adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and its rules, (2) review those compliance policies and procedures annually, and (3) designate a chief compliance officer who is responsible for administering the compliance policies and procedures. The rule is designed to protect investors by fostering better compliance with the securities laws. The collection of information under rule 206(4)–7 is necessary to help ensure that investment advisers maintain comprehensive internal programs that promote the advisers' compliance with the Advisers Act and its rules. The Commission's examination and oversight staff may review the information collected to assess investment advisers' compliance programs. Responses provided to the Commission pursuant to the rule in the context of the Commission's examination and oversight program are generally kept confidential. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number.

The respondents to this information collection are investment advisers registered with the Commission. Updated data indicate that there were 14,376 advisers registered with the Commission as of August 2021. Each respondent would produce one response, per year. Commission staff has estimated that compliance with rule 206(4)–7 imposes an annual burden of approximately 90 hours per response. Based on this figure, Commission staff estimates a total annual burden of 1,293,840 hours for this collection of information.

The public may view the background documentation for this information collection at the following website, *www.reginfo.gov.* Comments should be directed to: (1) Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10102, New Executive Office Building, Washington, DC 20503, or by sending an email to: *Lindsay.M.Abate@omb.eop.gov;* and (2) David Bottom, Director/Chief Information Officer, Securities and Exchange Commission, c/o John R. Pezzullo, 100 F Street NE, Washington, DC 20549 or send an email to: *PRA_Mailbox@sec.gov.* Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain.* Find this particular information collection by selecting "Currently under 30-day Review—Open for Public Comments" or by using the search function.

Dated: January 14, 2022.

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2022–01061 Filed 1–19–22; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

[SEC File No. 270–586, OMB Control No. 3235–0647]

Submission for OMB Review; Comment Request

Upon Written Request, Copies Available From: Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington, DC 20549–2736

Extension:
Rule 204

Notice is hereby given that pursuant to the Paperwork Reduction Act of 1995 ("PRA") (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission ("Commission") has submitted to the Office of Management and Budget ("OMB") a request for approval of extension of the previously approved collection of information provided for in Rule 204 (17 CFR 242.204), under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.*).

Rule 204(a) provides that a participant of a registered clearing agency must deliver securities to a registered clearing agency for clearance and settlement on a long or short sale in any equity security by settlement date, or if a participant of a registered clearing agency has a fail to deliver position at a registered clearing agency in any equity security for a long or short sale transaction in the equity security, the participant shall, by no later than the beginning of regular trading hours on the applicable close-out date, immediately close out its fail to deliver positions by borrowing or purchasing securities of like kind and quantity. For a short sale transaction, the participant must close out a fail to deliver by no later than the beginning of regular trading hours on the settlement day following the settlement date. If a participant has a fail to deliver that the participant can demonstrate on its books and records resulted from a long sale, or that is attributable to bona-fide market making activities, the participant must close out the fail to deliver by no later than the beginning of regular trading hours on the third consecutive settlement day following the settlement date. Rule 204 is intended to help further the Commission's goal of reducing fails to deliver by maintaining the reductions in fails to deliver achieved by the adoption of temporary Rule 204T, as well as other actions taken by the Commission. In addition, Rule 204 is intended to help further the Commission's goal of addressing

Examination Submission Form

Identify Protect Detect Respond Recover

Identify: Risk Assessments & Management	YES	NO	N/A
1. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices (e.g. frequent password changes, locking of devices, reporting of lost or stolen devices, etc.).			
2. The firm has an inventory of all hardware and software.			
Protect: Use of Electronic Mail	YES	NO	N/A
3. Email communications are secured. (If the response is no, proceed to the next question.) Current Regulatory Requirement on PPI Communications			
4. Employees and clients are aware that email communication is not secured.			
Protect: Devices	YES	NO	N/A
5. The investment adviser has written policies and procedures regarding the destruction of electronic data and physical documents.			
6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures. Current Regulatory Requirement			
Protect: Use of Cloud Services	YES	NO	N/A
7. The investment adviser has a back-up of all records off-site.			
8. The investment adviser allows remote access to its network (e.g. through use of VPN).			
Protect: Use of Firm Websites	YES	NO	N/A
9. The firm's website includes a client portal. [SURVEY QUESTION]			
Protect: Custodians & Other Third-Party Vendors	YES	NO	N/A
10. [Relevant to custodians only] The investment adviser has discussed with the custodian matters regarding the impersonation of clients and authentication of client orders.			
Protect: Encryption	YES	NO	N/A
11. The investment adviser utilizes encryption on all data systems that contain (or access) confidential information.			
Detect: Anti-Virus Protection and Firewalls	YES	NO	N/A
12. The investment adviser firm regularly uses anti-virus software on all devices accessing the firm's network, including mobile phones.			
13. Anti-virus updates are run on a regular and continuous basis.			
14. All software is scheduled for automatic updates.			
15. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events.			
16. A firewall is employed and configured appropriate to the firm's needs.			
Respond: Responding to a Cyber Event	YES	NO	N/A
Recover: Cyber-insurance	YES	NO	N/A
17. The investment adviser has considered whether cyber insurance is necessary or appropriate for the firm. [SURVEY QUESTION]			
Recover: Disaster Recovery	YES	NO	N/A
18. The investment adviser has a business continuity plan to implement in the event of a business outage/cybersecurity event.			
19. The investment adviser has a process for retrieving backed-up data and archival copies of information.			
20. The investment adviser has written policies and procedures for employees regarding the storage and archival of information.			

Firm Name _____ Firm CRD# _____

Designated Official Signature _____ Date _____

SAMPLE Use Google Form Link to Complete Submission