The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 6 June 17, 2015

FINANCIAL SERVICES

Model Cybersecurity Contract Terms and Guidance for Investment Managers to Manage Their Third-Party Vendors

By Robert R. Kiesel
Schulte Roth & Zabel

Like many companies, investment managers require a wide range of third-party vendor-provided products and services to manage their daily operations. These vendors have varying levels of access to sensitive data, and policies are needed to reduce the cybersecurity risks that third-party vendors present.

Typical agreements entered into by investment managers for products and services include administration agreements, prime brokerage and derivatives clearing agreements, trading system agreements, license agreements for investment analysis, risk management and portfolio valuation tools, market data agreements, software development agreements, hardware purchase agreements, website design agreements and consulting agreements. It is critical to have comprehensive contract provisions in place to reduce the risk that sensitive data of the managers and their investors will be stolen or inadvertently disclosed by or through third-party vendors.

In addition, investment managers that follow the foregoing guidelines when managing third-party vendors should be in compliance with the financial regulators' expectations regarding vendor management.

Regulators Alerting Managers of Vendor Cybersecurity Risks

SEC Focus on Cybersecurity

In April 2014, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert[1] announcing that it would conduct examinations of more than 50 registered broker-dealers and investment advisers focusing on "areas related to cybersecurity." In the Risk Alert, OCIE noted that businesses, including investment advisers, need to incorporate data security requirements into their contracts with third-party vendors to better protect investors and the capital markets from cyber threats.

The Risk Alert included "sample" requests for information that OCIE might "use in conducting examinations of registered entities regarding cybersecurity matters." Questions 16 through 20 of the Risk Alert covered the investment adviser's management of third-party vendors. The questions asked about the manager's cybersecurity risk assessment of vendors, training materials used for vendors, segregation of sensitive data from third-party access and security applied to control remote systems access by vendors.

In February 2015, OCIE reported the findings of its cybersecurity examinations.[2] Among other significant conclusions, OCIE's Risk Alert Follow-Up reported that few investment advisers are placing adequate cybersecurity requirements on the vendors that are granted access to the advisers' IT networks. Specifically:

- Only 32% of the examined sample of investment advisers required vendors with network access to conduct "cybersecurity risk assessments";[3]
- Only 24% "incorporate requirements relating to cybersecurity risk into their contracts" with such vendors;[4] and
- Only 13% had policies "related to information security training" for such vendors.[5]
- In contrast, the numbers for registered broker-dealers were much higher (84%, 72% and 51%, respectively).

On April 28, 2015, the SEC's Division of Investment Management issued a Guidance Update[6] that, among other things, stated "[b]ecause funds and advisers rely

on a number of service providers in carrying out their operations, funds and advisers may also wish to consider assessing whatever protective cybersecurity measures are in place at relevant service providers."

The SEC further noted that "[s]ervice providers may be given limited access to a fund's technology systems that may inadvertently enable unauthorized access to data held by the fund. Funds, as well as advisers, may wish to consider reviewing their contracts with their service providers to determine whether they sufficiently address technology issues and related responsibilities in the case of a cyber attack." See "*The SEC's Updated Cybersecurity Guidance Urges Program Assessments*," The Cybersecurity Law Report, Vol. 1, No. 3 (May 6, 2015).

The SEC's focus on cybersecurity is fairly new, but it seems heartfelt. Investment managers, in response, are wise to develop and document written vendor management policies to address cybersecurity risks posed by third-party vendors. These written policies should cover the areas addressed below.

CFTC Concerns and Attention

A growing number of investment managers are also registered with the U.S. Commodity Futures Trading Commission as commodity pool operators or commodity trading advisors. Mirroring the concerns of the SEC, the CFTC has held roundtables on Cybersecurity and System Safeguards Testing (with the most recent being held on March 18, 2015) and, in March 2014, issued guidance on data security (which set forth a clear expectation that CFTC registrants will enact cybersecurity safeguards and processes).[7]

The Diligence Process: Choosing a Vendor

The first step in responsibly choosing a third-party vendor is to investigate the proposed vendor, its creditworthiness, and the quality of its product or service prior to entering into a contract, especially if the vendor is not a household name. See "*Designing and Implementing a Three-Step Cybersecurity Framework for Assessing and Vetting Third Parties (Part One of Two)*," The Cybersecurity Law Report, Vol. 1, No. 1 (Apr. 8, 2015); *Part Two of Two*, Vol. 1, No. 2 (Apr. 22, 2015).

These investigatory steps should be added to the investment manager's information security policy in a separate vendor management section.

The best source of due diligence information about a vendor and its product may be other customers of the vendor. It is routine for vendors to offer customer references, and investment advisers should take advantage of these offers. The references offered by the vendor, however, will typically be its best references. It is therefore prudent for a manager independently to seek out other customers of the vendor who might not paint such a rosy picture. Trade organizations are a good source of information that can be used to find other vendor customers. The investment management community is a cooperative rather than competitive environment with respect to cybersecurity.

Investment advisers should ask for and review the vendor's written information security program, security incident response plan, business continuity plan, privacy policy and the results of any security audits previously conducted by the vendor. It is standard practice for the vendor to attach copies of its programs as exhibits to the vendor contract as contractual commitments of the vendor. A vendor's response to a request for these plans and policies can often be a barometer for that vendor's sophistication level regarding cybersecurity.

The vendor should also identify any subcontractors that will have access to the manager's sensitive information and should provide diligence material for each subcontractor.

Drafting Critical Contract Provisions

Exhibit A, below, provides a fairly comprehensive set of data security-related contract provisions that an investment manager can request its vendors incorporate into their contracts.

A manager's information security policy should include a vendor management section that requires the manager to attempt to obtain provisions substantially similar to the provisions outlined in Exhibit A in all agreements with third-party vendors that will be provided access to the manager's sensitive information and technology systems. These contract provisions cover, among other areas, the areas specifically mentioned by OCIE in the Risk Alert Follow-Up, namely, cybersecurity risk assessment and information security training.[8]

A sophisticated vendor, however, will not usually simply agree to be bound by the manager's suggested contract provisions. The vendor will have its own information security plans, as tailoring its security infrastructure to meet the requirements of every customer could be overly burdensome. In this case, the manager should review the vendor's plans and require the vendor to be bound by those. As long as the vendor's plans are reasonable, and reasonably comprehensive, agreeing to use the vendor's terms should not cause the manager any compliance problems.

Unsophisticated vendors, such as small IT consulting shops, may not be familiar with all of the various facets of a comprehensive data security plan. If the manager nonetheless wants to work with the vendor, the manager should review Exhibit A's provisions in detail with the vendor to make sure the vendor can comply with them. If not, it may be best to obtain the services of another vendor.

More Limited or Specific Access

The provisions in Exhibit A relate to vendor-hosted services when the vendor will have technological access to the manager's sensitive data. Other contract provisions can be tailored by the manager to apply to scenarios where vendors will have more limited access.

Representation for Sensitive Data Access Only

For example, if a vendor will not be provided IT system access but will otherwise have access to a manager's sensitive data, it should be sufficient to obtain a representation as follows:

> Vendor has (1) a written information security policy (WISP); (2) a written business continuity plan (BCP); (3) a written vendor management policy (VMP); and (4) a published privacy policy (Privacy Policy and together with WISP, BCP and VMP, Data Security Policies) (such Privacy Policy governing the collection and use of "nonpublic personal information" (as defined in the Privacy Policy) (together with the Manager's and its investors' other sensitive data, "Customer Information") that discloses the manner by which it collects, uses and transfers Customer Information).
>
> Vendor has provided to Manager copies of its Data Security Policies. Vendor will not allow the release of any Customer Information and will not violate any of its Data Security Policies or allow any person to gain unauthorized access to or make any unauthorized use of any Customer Information.

Product Security Representation

If, on the other hand, a vendor will not have access to the manager's systems and will not have access to the manager's sensitive data, it will still be important to obtain a representation specific to the security of the vendor's product. For example, if the manager is licensing third-party software, the use of which by itself could cause security risks, a basic product-specific representation such as the following should be used:

> Vendor has processes and checks in place to ensure that its [software/website/service] is free from viruses and similar defects. The [software/website/service] does not contain any virus, Trojan horse, worm, time bomb or other computer programming routine, device or code that could reasonably be anticipated to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or information. The [software/website/service] does not contain any malware, backdoor or other technological routine,

device or code that could adversely affect the security or confidentiality of Manager's systems or data.

Other Key Vendor Provisions

The vendor should agree to obey any specific instructions the manager provides with respect to the manager's or its investors' data, including in connection with any litigation or regulatory holds, and in connection with any termination or expiration of the vendor contract.

The vendor should agree to provide transition services in connection with the termination or expiration of the vendor contract to allow the manager to obtain a safe return of its data, or to transition the data to another vendor.

Additionally, the vendor should covenant that it will provide access to the manager's sensitive data only to vendor's employees and subcontractors that need access to the information to perform their respective jobs in connection with the vendor's product or service (and only to the extent of such need); have agreed to be bound by confidentiality and security provisions at least as strict as those agreed to by the vendor; and in the case of subcontractors, have provided due diligence information to the manager of the type delivered by the vendor (i.e., WISP, security incident response plan, BCP, privacy policy and results of security audits).

The vendor should also agree to be responsible for its subcontractors (or, at least, to have selected them with due care, supplemented by an at-least-annual review).

Limiting Vendor Access

A fairly obvious technological step to limit the security exposure risk a manager has to a third-party vendor is to limit the systems and sensitive data access provided to the vendor to a need-to-access basis. Limiting the vendor's access to the manager's systems limits the damage that can be done if an attacker gains access to the vendor's sensitive data (which could include the manager's sensitive data in the vendor's possession), or if a vendor employee steals the vendor's (and/or manager's) data.

For example, a client relationship management service vendor would probably need access to sensitive investor data but should not have access to sensitive data it does not need to use, such as trading algorithm software or a manager's internal emails. Alternatively, a trading system software vendor may need access to the manager's proprietary trading software but should not have access to any investor information or internal emails.

Payment Authorizations

Many external threats to investment managers seek to trick the manager's employees into sending money to the source of the threat. Adopting reasonable multi-tier payment approvals can lessen this risk.

For example, a creative and common spear-phishing attack is one in which the attacker figures out from one or more sources that a manager is a customer of a particular vendor, such as an IT equipment seller. The attacker pretends to be a purchasing employee of the manager and orders equipment from the vendor on the manager's account. The vendor is instructed to ship the equipment to the attacker and the manager gets the invoice.

To fight this and several other types of phishing attacks, multiple levels of internal approvals should be required to authorize the payment of trade accounts, and at some level of the process, an employee should verify the actual delivery of the invoiced products and services, and confirm that the invoiced amounts are actually owed to the vendor. Use of a multi-tiered approval system will make it more difficult for an attacker to bypass the necessary steps to divest the manager's funds.

Robert Kiesel is chair of SRZ's Intellectual Property, Sourcing & Technology Group and Vendor Finance Group and co-head of its Cybersecurity Group. His practice focuses on the preparation and negotiation of various

types of commercial agreements, including agreements for information technology transactions; equipment finance and leasing transactions with an emphasis on vendor finance programs; and the financing of computer hardware and software and manufacturing equipment. He also handles supply agreements for components and finished goods, as well as "take-or-pay" agreements, joint engineering, research and development relationships, and technology-sharing arrangements. Kiesel works on a broad range of services agreements as well, including transition and long-term services in mergers and acquisitions transactions. SRZ's Cybersecurity Group works with the world's top alternative asset managers, financial institutions and companies operating across a broad range of industries in managing the risks associated with data protection and privacy laws.

* * *

Exhibit A: Sample Vendor Contract Provisions

[This sample only applies to vendor-hosted services containing sensitive manager data.]

I. General

Vendor has examined Manager's current computer networking platform and its hosting and data security requirements to the extent Manager has provided Vendor access, and confirms that the Vendor's Service will interact and operate with the Manager's platform and provide a secure hosting environment in accordance with the specifications and in accordance with industry standards for the protection of confidential information. If the agreement between the Vendor and the Manager is terminated or expires, Manager shall have the option to replace the Vendor with a third-party provider of its choosing, and Vendor shall undertake commercially reasonable efforts to transition Manager to the new provider as quickly, economically and efficiently as possible and will do so in a way that provides a seamless and secure transition with no business interruptions to Manager.

II. Security

A. Application Security

Vendor shall implement the following best practices with regard to development and deployment of the Vendor's Service.

Vendor shall maintain appropriate systems security for the Vendor's Service in accordance with commercially reasonable industry standards and practices designed to protect all data and information provided by or on behalf of Manager that is input into, displayed on or processed by the Vendor's Service and all output therefrom ("Manager Data") from theft, unauthorized disclosure and unauthorized access. Such systems security includes, among other things: (1) implementation of application vulnerability tests and provision to Manager of evidence of tests and results; (2) all Vendor-Manager communications to or through the web security layer will be transmitted using a robust secure protocol; and (3) the following safeguards:

1. *Authentication*

   a) All access is authenticated and communication secured using industry best practices.

   b) Systems identity is tied to an individual user by the use of credentials and by second factor authentication.

   c) Reasonable authentication controls that conform to industry recognized standards are provided.

2. *Authorization*

   Vendor agrees to:

   a) Ensure that authorized users are only allowed to perform actions within their privilege level.

b) Control access to protected resources based upon role or privilege level.

c) Prevent privilege escalation attacks.

3. *Secure Coding Practices*

a) Developers should be trained on secure developing best practices.

b) Applications should be written in a secure manner using a formal process that provides evidence that application security vulnerabilities are not present prior to moving into production and periodically thereafter, including after significant changes. At a minimum, application security vulnerabilities would include the SANS Top 20 and OWASP Top 10.

c) These requirements should be validated by tools such as dynamic application scanning and/or static code analysis.

4. *Password and Account Management*

a) Passwords should follow best practices, including:

i. Encrypting passwords using "hashing" and "salting" techniques.[9]

ii. Enforcing password complexity.

iii. Limiting failed attempts before account lockout.

iv. Not allowing clear passwords.

v. Password reset does not send credentials.

b) Where appropriate, Vendor shall securely log (with time and date) commands requiring additional privileges to enable a complete audit trail of activities.

B. Data Security

Vendor shall implement the following best practices:

1. *Data at Rest*

a) Manager Data is encrypted using industry best practices.

b) Backups of Manager Data have the same controls as production data.

2. *Data in Motion*

a) Manager Data in transit to or from Manager will be encrypted (e.g., SFTP, certificate-based authentication).

b) Manager Data sent over browser should use SSLv3 or better.

3. *Multi-Tenancy*

a) In a multi-tenant environment, Vendor shall provide appropriate security controls and robust cryptographic methods to protect and isolate Manager Data from other tenants.

4. *Administrative Access and Environmental Segregation*

a) Applying Principle of Least Privilege: Proper controls should be in place to ensure that access is limited to administrators who must see Manager Data in order to fulfill their job functions.

b) Where possible, confidential data should be masked with one-way hashing algorithms.

c) Manager Data should not be replicated to non-production environments.

C. Threat Management

Vendor shall implement the following best practices:

1. *Intrusion Detection*

Vendor shall implement and maintain an intrusion detection monitoring process at the network and host level to protect the Vendor's Service and to detect unwanted or hostile network traffic. Vendor shall update its intrusion detection software continuously, on a scheduled basis following the availability of updates by the software provider. Vendor shall implement measures to ensure that Vendor is alerted when the system or service detects unusual or malicious activity. Vendor shall notify Manager within three (3) days of any significant intrusion.

2. *Penetration Tests*

Manager has the right to perform, or to have a third party perform, independent intrusive application penetration tests on its segmented data and directories of the Vendor's Service infrastructure at Manager's own expense, no more than twice per year, and Vendor shall reasonably facilitate the same. In addition, Vendor shall conduct penetration tests at least once per year on its manager-wide computing environment and will provide Manager with written copies of the results of such penetration tests performed by Vendor or its subcontractors no more than thirty (30) days after Vendor obtains the results or reports.

D. Infrastructure Security

Vendor shall configure the infrastructure (e.g., servers and network devices) and platforms (e.g., OS and web servers) to be secure following these best practices:

1. *Audit Logging*

a) Vendor shall monitor and log all system access to the Vendor's Service to produce an audit trail that includes, but is not limited to, web server logs, application logs, system logs and network event logs.

b) The logs should be stored off-system to reduce risk of loss due to tampering.

2. *Network Security*

a) Vendor shall comply with industry standards, separating perimeter networks from endpoints hosted in the private network using industry standard firewalls. Vendor shall update its firewall software continuously, on a scheduled basis, following the availability of updates by the software provider.

b) Vendor shall test its perimeter devices continuously on a scheduled basis, and, if deficiencies are discovered, Vendor shall promptly troubleshoot and remediate security deficiencies discovered as a result of such testing or as a result of logging access attempts, based upon the risk of the deficiency.

3. *Vulnerability Management*

In addition to the third-party vulnerability assessments described above, Vendor shall implement commercially reasonable processes designed to protect Manager Data from system vulnerabilities, including:

a) Perimeter Scanning: Vendor shall perform perimeter scanning through the use of embedded adaptors within Vendor's infrastructure providing information to an external reporting tool. Vendor shall produce reports monthly and make them available to Manager upon written request.

b) Internal Infrastructure Scanning: Vendor shall perform internal infrastructure scanning through the use of embedded adaptors within Vendor's infrastructure providing information to an external reporting tool through a

VISA-approved PCI scanning vendor. Vendor shall produce reports monthly and make them available to Manager on a monthly basis upon written request.

c) Application Vulnerability Scanning: Vendor shall perform application vulnerability scanning on the Vendor's Service before code is released into production. Vendor shall produce reports reasonably promptly thereafter and make them available to Manager on request.

d) Malware Scanning: Vendor shall perform anti-malware scanning on all servers utilized in performing the Vendor's Service.

4. *Secure Configuration*

Vendor shall comply with industry standards for platform hardening and secure configuration in order to reduce attack scope and surface. Hardening procedures should be enforced before any system is put into production.

E. Security Procedures

Vendor shall implement the following best practices:

1. *Incident Response*

Vendor shall maintain security incident management policies and procedures, including detailed security incident escalation procedures. In the event of a breach of any of Vendor's security or confidentiality obligations, Vendor agrees to notify Manager by telephone and email of such an event within twenty-four (24) hours of discovery. Vendor will also promptly perform an investigation into the breach, take appropriate remedial measures and provide Manager with the name of a single Vendor security representative who can be reached with security questions or security concerns twenty-four (24) hours per day, seven (7) days per week, during the scope of Vendor's investigation.

2. *Patch Management*

Vendor shall use a patch management process and tool set to keep all servers up to date with appropriate security and feature patches.

3. *Documented Remediation Process*

Vendor shall use a documented remediation process designed to timely address all identified threats and vulnerabilities with respect to the Vendor's Service. High severity findings should be reported to Manager and remediated within thirty (30) days.

4. *Employee Termination Procedures*

Vendor shall promptly terminate all credentials and access to privileged password facilities of a Vendor employee in the event of termination of his or her employment.

F. Governance

Vendor shall implement the following best practices:

1. *Security Policy*

Vendor shall maintain a written information security policy that is approved annually by Vendor and published and communicated to all Vendor employees and relevant third parties. Vendor shall maintain a dedicated security and compliance function to design, maintain and operate security in support of its "trust platform" in line with industry standards. This function shall focus on system integrity, risk acceptance, risk analysis and assessment, risk evaluation, risk management and treatment statements of applicability and vendor management.

2. *Security Training*

Vendor shall ensure, at no expense to Manager, that all Vendor employees and managers complete

relevant training required to operationalize the procedures and practices outlined herein, including security awareness training, on at least an annual basis. Vendor shall provide evidence of training to Manager when completed.

3. *Security Reviews*

Senior-level managers of Manager and Vendor shall meet at least once annually to discuss: (1) the effectiveness of the Vendor's security platform; and (2) any updates, patches, fixes, innovations or other improvements made to electronic data security by other commercial providers or for other customers of Vendor that Vendor or Manager believe will improve the effectiveness of the Vendor's security platform for Manager.

4. *Third-Party Audits and Compliance Standards*

a) Vendor shall provide Manager with a copy of any security audit (including SSAE 16, AICPA Service Organization Control Reports or independent audits) that is performed no more than thirty (30) days after Vendor receives the results or reports. Manager has the right to, or to engage a third party on its behalf to, visit Vendor's offices up to four (4) times per calendar year in order to conduct due diligence and auditing procedures on Vendor's business operations related to the Vendor's Service in terms of technical infrastructure, system interaction, organization, quality, quality control, personnel involved with services for Manager, and general resources in terms of skills and personnel.

b) Vendor will furnish evidence of a successful SSAE 16 audit upon Manager request to the extent permitted by law and subject to applicable regulatory restrictions and confidentiality obligations. Vendor must verify that the audit certifies all infrastructure and applications that support and deliver services to Manager Data.

c) Vendor will furnish evidence of a successful ISO 27001 audit upon Manager request to the extent permitted by law and subject to applicable regulatory restrictions and confidentiality obligations. Vendor must verify that the audit certifies all infrastructure and applications that support and deliver services to Manager Data.

d) [PCI-DSS COMPLIANCE IF APPLICABLE]

Vendor shall maintain policies, practices and procedures sufficient to comply with the Payment Card Industry Data Security Standard, as the same may be amended from time to time, with respect to the Vendor's Service.

e) Vulnerability Assessments

At least annually, Vendor shall conduct an application vulnerability assessment with respect to the handling of data relating to the Vendor's Service, which assessment will be performed by a qualified independent third party. Upon Manager's request, Vendor shall provide Manager with copies of documentation relevant to such assessment to the extent permitted by law and subject to applicable regulatory restrictions and confidentiality obligations.

G. Physical Security

Vendor shall implement the following best practices:

Vendor shall limit access to its facilities utilized in performing the Vendor's Service to employees and employee-accompanied visitors using commercially reasonable Internet industry standard physical security methods. At a minimum, such methods shall include visitor sign-ins, restricted access key cards and locks for employees; limited access to server rooms and archival backups; and burglar/intrusion alarm systems.

H. Business Continuity

Vendor shall implement the following best practices:

1. Vendor shall have a business continuity plan in place for the restoration of critical processes and operations of the Vendor's Service at the location(s) from which the Vendor's Service is provided. Vendor shall also have an annually tested plan in place to assist Vendor in reacting to a disaster in a planned and tested manner. Vendor shall provide Manager with a copy of its then-current plan promptly following Manager's written request for same. Such a plan must differentiate between a failure that is contained within an applicable data center (Type A Incident) and a failure in which an entire applicable data center is not available (Type B Incident). Key features and goals of the plan shall include:

a) Recovery Point Objective

Backup state frequency up to one (1) hour of user data in a Type A Incident and up to twenty-four (24) hours in a Type B Incident.

b) Recovery Time Objective

i) Recovery time objective is three (3) hours after a critical system malfunction is detected. Up to one (1) hour assigned for attempting to fix existing conditions without resorting to full disaster recovery procedure and two (2) additional hours for full disaster recovery.

ii) Vendor shall provide notification to Manager for any disaster that causes the Vendor's Service to be down and unavailable within thirty (30) minutes of such disaster. Within one (1) day after such disaster, Vendor will recover the Vendor's Service and Manager Data.

iii) If Vendor's business continuity plan is invoked: (1) Vendor shall execute such plan and restore the Vendor's Service to the applicable service availability service level; and (2) Manager shall be treated with at least equal priority as any other Vendor customer.

2. *Backup Management*

a) Vendor shall perform full backups of the database(s) containing Manager Data no less than once per day without interruption of the Vendor's Service. Vendor shall also provide off-site archival storage on no less than a weekly basis of all backups of the database(s) containing Manager Data on secure server(s) or other commercially acceptable secure media. Such data backups will be encrypted, sent off-site to a secure location each business day and stored/retained for seven (7) years.

b) In order to recover from a Type B Incident, the required backed-up data will be replicated over at least three (3) geographically dispersed data centers at any point in time. Backup snapshots may be periodically sent to another data center. Data retention for a Type A Incident will utilize twenty-four (24) hourly snapshots, fourteen (14) daily snapshots and three (3) monthly snapshots. This backup policy is designed to allow for a partial restoration of the system as well as a full system restoration.

3. *Right to Audit*

Manager has the right to, or to engage a third party on its behalf to, at its own expense, visit Vendor's offices once per calendar year in order to conduct due diligence and auditing procedures on Vendor's business operations related to the Vendor's Service in terms of technical infrastructure, systems interaction, organization, quality, quality control, personnel involved with services for customers, and general resources in terms of skills and personnel.

[1] Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (April 15, 2014) (Risk Alert).
[2] Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Examination Sweep Summary (Feb. 3, 2015) (Risk Alert Follow-Up).
[3] Risk Alert Follow-Up at 2.
[4] Id. at 4.
[5] Id.
[6] Securities and Exchange Commission, Division of Investment Management, IM Guidance Update No. 2015-02, Cybersecurity Guidance (April 2015) (Guidance Update).
[7] Division of Swap Dealer and Intermediary Oversight, CFTC Staff Advisory No. 14-21 (Gramm-Leach-Bliley Act Security Safeguards).
[8] They are also intended to satisfy the best practices criteria in the CFTC guidance, which states: "To the extent that third party service providers have access to customer records and information, [a manager should] . . . [c]ontractually requir[e] service providers to implement and maintain appropriate safeguards."
[9] "Hashing" a password converts it into a long hexadecimal number. "Salting" is the addition of random characters to the password before it is hashed. The idea is that this is difficult to decode, especially with added "salt." Thus, even if a password file itself is compromised, it still has a certain level of protection and individuals have some time to change their passwords before they are decoded.

