OCIE Risk Alert: Cybersecurity: Ransomware Alert

On July 10, 2020, the Office of Compliance Inspections and Examinations (OCIE) released a Risk Alert highlighting the dangers of ransomware to SEC-registered entities, including investment advisers. The Risk Alert is a response to a marked uptick in both the prevalence and sophistication of ransomware attacks in recent months. Ransomware is a type of malware used by criminals to gain control of your or your firm's confidential information and customer data. In order to regain control and/or maintain confidentiality, victims are generally required to pay some form of ransom to the perpetrators. For obvious reasons, it is important for all firms to take proper security measures to protect against such attacks.

Each firm is different and so are their security measures, however OCIE has identified several areas of concern that all firms need to be aware of:

Incident response and resiliency policies, procedures and plans.

Firms should be continually assessing, testing, and periodically updating their incident response and resiliency policies, procedures and plans, such as contingency and disaster recovery plans. Possible areas to look at include procedures for timely notification, escalation policies, as well as state and federal notification requirements.

NEXT

Operational Resiliency.

It is important to identify which systems and processes can be brought back online during a disruption, allowing business operations to continue.

Awareness and training programs.

Firms should be providing up-to-date targeted cybersecurity training, such as education and exercises on phishing to help employees identify such threats. This training should be administered firm-wide, as all employees are potential entry points for hackers.

Vulnerability scanning and patch management.

It is vital that firms work with their software providers to keep their cybersecurity software up to date and install all security patches.

Access management.

Maintaining secure access to information, both online and in the real world should be a priority for all firms. Examples of this include allowing employees only as much access as necessary to perform their jobs, utilizing multi-factor authentication wherever possible, and requiring at least annual recertification for users' access rights.

Perimeter security.

Firms should utilize system-wide perimeter security to monitor all incoming and outgoing traffic to protect against dangerous or unwanted traffic, such as the use of firewalls and enabling email security features.

Finally, OCIE points to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) as an additional resource for firms. CISA publishes cybersecurity alerts that firms should be aware of, and encourages firms to share them with their third-party service providers.

CISA Alert: https://www.us-cert.gov/ncas/alerts/aa19-339a
OCIE Risk Alert: https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf

OCIE Risk Alert: Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers

In response to the ongoing disruption caused by COVID-19, OCIE issued a Risk Alert on Aug. 12, 2020. In the Risk Alert, OCIE makes various observations and recommendations which fall into six different categories: (1) protection of investors' assets; (2) supervision of personnel; (3) practices relating to fees, expenses, and financial transactions; (4) investment fraud; (5) business continuity; and (6) the protection of investor and other sensitive information. In the Risk Alert, OCIE discusses these categories and how difficulties such as a remote work environment, market upheaval, and bad actors attempting to take advantage of the situation may affect investment advisers in different ways.

Protection of Investor Assets

In light of the current operating environment, OCIE has observed that some firms have modified their normal operating procedures regarding collecting and processing investor checks and transfer requests. Firms may wish to review their practices and consider disclosing to clients that checks or other documents mailed to the firm office location may experience delays in processing. Also, firms may want to consider revisions to policies and procedures regarding assistance with disbursements, including where investors are taking unusual or unscheduled withdrawals from their accounts. These policy and procedure revisions may include additional steps to validate the identity of a client and distribution instructions, as well as recommending that clients have in place a trusted contact.

Supervision of Personnel

With personnel working from home for extended periods, supervisors are likely not having the same level of oversight and interaction with personnel working remotely. In addition, firms should be cognizant of the heightened risk of fraud, limitations of onsite due diligence and other constraints in reviewing third-party managers. Furthermore, firms should be cognizant of communications occurring outside of a firm's systems due to a remote work environment.

Fees, Expenses and Financial Transactions

Market volatility and other factors may increase financial pressures on firms, which may increase incentives for misconduct relating to fees and expenses charged to clients. OCIE references possible failures by firms relating to fee calculation errors resulting in overbilling, failures to provide breakpoints and aggregating accounts, and failures to refund prepaid fees for terminated accounts.

Investment Fraud

Due to the various travel, meeting and related restrictions, OCIE is cognizant of increased risk of fraud in conducting due diligence on investments and in determining if investments are suitable for firm clients.

Business Continuity

Due to the move by many firms to remote operations, OCIE recommends firms review compliance policies and procedures to determine if revisions are necessary. In addition, firms should consider reviewing support facilities and remote sites to determine: if additional resources and/or measures for securing servers and systems are needed; the integrity of vacated services is maintained; and remote location data is protected.

Protection of Investor and Other Sensitive Information

A remote work environment and the use of tools such as video conferencing and other electronic means of communicating may provide enhanced opportunities for the compromise of confidential customer information. OCIE notes the following concerns relating to a remote work environment: the use of personally owned devices; documents printed at remote locations; and increased phishing opportunities. In response to these increased risks, OCIE recommends that firms review their policies and procedures to consider:

- Enhancements to identity theft protection practices;
- Providing to personnel additional training regarding phishing, sharing information while working remotely, encryption and destruction of physical documents;
- Conducting heightened reviews of personnel access rights and controls as personnel may take on expanded responsibilities;
- Utilizing encryption technologies; and
- To the extent available, enhanced system access security, such as dual authentication.

https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf

OCIE Risk Alert: Cybersecurity: Safeguarding Client Accounts against Credential Compromise

OCIE's most recent Risk Alert, published Sept. 15, 2020, address another cybersecurity issue, this time highlighting the dangers of "credential stuffing." Credential stuffing is a method of cyberattack that uses compromised client login credentials and can lead to loss of customer assets and the disclosure of confidential or other personal information. Hackers will obtain groups or lists of usernames, email addresses, and their passwords from sellers on the dark web. They then attempt to use these compromised usernames and passwords from the original site to gain access to other websites. If successful, this process can enable bad actors to access a firm's customer accounts. If undetected, these attacks can eventually allow hackers to gain access to firms' systems and steal assets from customer accounts, access confidential information as well as additional login credentials/website information which can be resold to others on the dark web.

According to OCIE, there has been a recent increase in the prevalence of such attacks. OCIE is urging firms to take proactive steps to mitigate the risks of credential stuffing. OCIE has identified two of the largest online behaviors that lead to successful attacks, which are (1) individuals using the same password or minor variations of the same password for various online accounts, and/or (2) individuals using login names that are easily guessed, such as email addresses or full names.

As stated above, firms should be proactive in their efforts to combat credential stuffing. Some of the methods referenced by OCIE for consideration by firms include:

- Periodic review and updating of password policies or requiring a minimum password strength;
- Multi-factor authentication;
- Using systems that require a user to perform an action to prove they are human, like clicking on each picture of a car;
- Monitoring for higher-than-usual login attempts;
- Informing and educating clients on the importance of password construction, maintenance and protection; and
- Ensuring that if employee mobile phones are no longer operative, or if a number is transferred, that multi-factor authentication no longer utilizes these mobile phones.

https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf

SEC Enforcement Action: VALIC Financial Advisors

On July 28, 2020, the SEC announced a pair of settled administrative actions against Houston-based VALIC Financial Advisors (VFA).

In the first action, the SEC charged VFA with failing to disclose that its parent company paid a for-profit entity owned by a Florida teacher's union to promote VFA to Florida teachers. The second action involved VFA's wrap fee arrangements with clients.

In regards to the second action wrap fee arrangements, VFA instructed a third-party adviser to select from mutual funds in the no-transaction fee program offered by VFA's clearing firm. The selection of no-transaction fee funds provided various financial benefits to VFA. First, VFA's agreement with the clearing firm provided VFA with a portion of the revenue the clearing firm received from the mutual fund sponsor and any 12b-1 fees paid on client mutual fund assets. There were many 12b-1 fee-paying mutual fund share classes in the no-transaction fee program. In most instances, the mutual funds the third-party adviser selected had a lower-cost share class available that did not pay 12b-1 fees or that would not have led to revenue sharing to VFA. Second, by instructing the third-party adviser to limit new funds to those in the no-transaction fee program, VFA avoided paying execution costs for the clients' purchases or sales of the mutual funds in the no-transaction fee program. VFA did not disclose that it had provided this instruction to the third-party adviser or the conflicts of interest arising from this instruction.

VFA's activities as detailed in each action generally constituted violations of the anti-fraud provision of the Investment Advisers Act of 1940, specifically Section 206. In settlement of the first action, VFA agreed to a cap on its management fee for the advisory product made available to Florida teachers, as well as a $20,000,000 civil monetary penalty. In the second action, VFA had already rebated approximately $2.3 million in 12b-1 fees plus interest to affected clients. In addition, VFA was subject to disgorgement and prejudgment interest, and a civil monetary penalty in a total amount of $19,943,753.

https://www.sec.gov/litigation/admin/2020/34-89405.pdf
https://www.sec.gov/litigation/admin/2020/34-89407.pdf

SEC Roundtable to Discuss Reg BI and Form CRS

The SEC has announced it will host a roundtable of SEC and FINRA staff to discuss initial observations on Regulation Best Interest and Form CRS implementation. The roundtable, which will be held virtually, will take place Oct. 26, 2020, and discuss how firms have met the new rules and requirements since the compliance deadline. According to SEC Commissioner Caroline Crenshaw, two main areas of concern are making sure firms are held accountable when they fail to properly mitigate conflicts of interest, and that Form CRS actually provides "valuable" information to clients or potential clients. Another area which will likely be discussed is whether firms are properly disclosing legal and disciplinary history on Form CRS.

https://www.sec.gov/news/press-release/2020-229

BACK

RETURN TO TOP

Questions? Contact the DCS Team

Dinsmore Compliance Services (DCS), an affiliate of Dinsmore & Shohl LLP, offers compliance solutions for investment managers and municipal advisers. DCS will help you develop and maintain high-quality compliance programs customized to your particular business demands and operational realities. We offer these services, all as an affiliate of a coast-to-coast, full-service law firm.

Kevin Woodard
President
(513) 977-8646
kevin.woodard@dinsmorecomplianceservices.com

Jeff Chapman
Director of Client Relations
(513) 977-8647
jeff.chapman@dinsmorecomplianceservices.com

dinsmorecomplianceservices.com