Schulte Roth&Zabel
Private Funds Regulatory
UPDATE

SEC Provides Observations on "Credential Stuffing" Cyberattacks

October 2020

On Sept. 15, 2020, OCIE issued a cybersecurity Risk Alert[1] warning about an increase in cyberattacks against registered investment advisers and broker-dealers using "credential stuffing." Based on recent examinations, OCIE has observed that credential stuffing is an increasingly effective method of attack that can be used to steal assets from customer accounts and access sensitive information.

What is credential stuffing?

Credential stuffing is a type of cyberattack perpetrated by collecting compromised client login credentials from the dark web and, through the use of automated scripts, employing those credentials to gain unauthorized access to customer accounts and firm systems. These attacks are more effective than more traditional means, such as trying to guess passwords by attempting all of the words in a dictionary, because attackers are able to leverage specific information collected online, such as user names, email addresses and associated passwords. If successful, a cybercriminal gains access to a firm's accounts and systems, enabling the theft of assets from customer accounts and access to confidential information (including additional login credential information) and network resources. Information obtained by the attacker could be sold to other cybercriminals on the dark web. Bad actors may even monitor or take control of a customer's or employee's account.

OCIE observed that internet-facing websites — sites that are accessible to the public as opposed to sites that may only be access internally — are most vulnerable. This often includes sites hosted by third-party vendors. The presence of personal information on easily located internet-facing sites, such as the email address of a CTO, can also be combined with information retrieved from the dark web to obtain unauthorized access to accounts.

What steps should managers take to safeguard accounts and systems against credential stuffing?

OCIE encourages fund managers to be proactive in mitigating the risk of credential stuffing, including:

- *Password Policies and Procedures*. Periodic review of policies and programs with a specific focus on updating password policies to incorporate a recognized password standard requiring strength, length, type and change of passwords practices that are consistent with industry

[1] *See* Cybersecurity: Safeguarding Client Accounts against Credential Compromise (Sept. 15, 2020), available here.

standards. OCIE has observed that successful attacks occur more often when (1) individuals use the same password or minor variations of the same password for different online attacks; or (2) using login usernames that are easily guessed;

- *Multi-Factor Authentication ("MFA")*. Use of MFA to authenticate the person seeking to log in to an account, which can offer one of the best defenses to password-related attacks and significantly decrease the risk of an account takeover. As MFA frequently relies on sending data to mobile devices, OCIE warns of the need to be alert to when devices are lost or no longer working;
- *CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)*. Deployment of CAPTCHAs, which requires users to enter information to verify that they are not bots, frustrates the use of automated scripts used in credential stuffing;
- *Controls to Detect and Prevent*. Implementation of controls to detect and prevent credential-stuffing attacks. For example, monitoring for a higher than usual number of login attempts or implementing a Web Application Firewall ("WAF") that can identify and thwart credential stuffing attacks);
- *Dark Web Monitoring*. Surveillance of the dark web for lists of leaked user IDs and passwords; and
- *Training*. Educate employees and customers on the use of strong, unique passwords and on potentials signs of an attempted or successful cyberattack.

*This article appeared in the October 2020 edition of SRZ's Private Funds Regulatory Update. To read the full Update, **click here**.*