RISK ALERT
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

September 15, 2020

Cybersecurity: Safeguarding Client Accounts against Credential Compromise

I. Introduction

This Risk Alert highlights “credential stuffing” — a method of cyber-attack to client accounts that uses compromised client login credentials, resulting in the possible loss of customer assets and unauthorized disclosure of sensitive personal information.

The Office of Compliance Inspections and Examinations (“OCIE”) has observed in recent examinations an increase in the number of cyber-attacks against SEC-registered investment advisers (“advisers”) and brokers and dealers (“broker-dealers,” and together with advisers, “registrants” or “firms”) using credential stuffing. Credential stuffing is an automated attack on web-based user accounts as well as direct network login account credentials.[1] Cyber attackers obtain lists of usernames, email addresses, and corresponding passwords from the dark web[2] and then use automated scripts to try the compromised user names and passwords on other websites, such as a registrant’s website, in an attempt to log in and gain unauthorized access to customer accounts.

Credential stuffing is emerging as a more effective way for attackers to gain unauthorized access to customer accounts and/or firm systems than traditional brute force password attacks.[3] When a credential stuffing attack is successful, bad actors can use the access to the customer accounts to gain access to firms’ systems, where they are able to steal assets from customer accounts, access confidential customer information, obtain login credential/website information that they can sell to other bad actors on the dark web, gain access to network and system resources, or monitor and/or take over a customer’s or staff[4] member’s account for other purposes.

[1] The views expressed herein are those of the staff of OCIE. This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the “SEC” or the “Commission”). The Commission has neither approved nor disapproved the content of this Risk Alert. This Risk Alert has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by OCIE staff and is not legal advice.

[2] The “dark web” is a subset of the Internet, oftentimes used anonymously, that can only be accessed using specialized software.

[3] A “brute force” attack is an attempt to guess a password using numerous combinations, such as attempting all of the words in a dictionary.

[4] The term “staff” includes firm employees and contractors.

II. Summary of Observations

OCIE staff has observed an increase in the frequency of credential stuffing attacks, some of which have resulted in the loss of customer assets and unauthorized access to customer information. The failure to mitigate the risks of credential stuffing proactively significantly increases various risks for firms, including but not limited to financial, regulatory, legal, and reputational risks, as well as, importantly, risks to investors.

Firms' information systems, particularly Internet-facing websites, face an increased risk of a credential stuffing attack. This includes systems hosted by third-party vendors. Firms' Internet-facing websites are vulnerable to attack because they can be used by attackers to initiate transactions or transfer funds from a compromised customer's account. In addition, Personally Identifiable Information (PII) is often available via firms' Internet-facing websites. Obtaining a customer's PII from one firm's website can facilitate an attacker's ability potentially to take over a customer account or attack accounts held by the account owner at other institutions.

Successful attacks occur more often when (1) individuals use the same password or minor variations of the same password for various online accounts, and/or (2) individuals use login usernames that are easily guessed, such as email addresses or full names.

OCIE encourages registrants to consider reviewing and updating their Regulation S-P and Regulation S-ID policies and programs to address the emergent risk of credential stuffing.[5]

III. Firms' Response to Credential Stuffing

OCIE observed a number of practices that firms have implemented to help protect client accounts, including:

- Policies and Procedures. Periodic review of policies and programs with specific focus on updating password policies to incorporate a recognized password standard[6] requiring strength, length, type, and change of passwords practices that are consistent with industry standards;

- Multi-Factor Authentication ("MFA"). Use of MFA,[7] which employs multiple "verification methods" to authenticate the person seeking to log in to an account. The strength of authentication systems is largely determined by the number of factors

[5] Regulation S-P requires firms to adopt written policies and procedures that address certain safeguards for the protection of customer records and information. Regulation S-ID prescribes certain requirements for firms to establish identity theft preventions programs. *See generally*, 17 CFR 248.30(a) and 248.201.

[6] *See e.g.*, NIST Information Technology Laboratory- Computer Security Resources Center, SP 800-63-3 Digital Identity Guidelines, available at https://csrc.nist.gov/publications/detail/sp/800-63/3/final.

[7] NIST Information Technology Laboratory/Applied Cybersecurity Division, "Back to Basics: Multifactor Authentication (MFA), available at https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

incorporated by the system — the more factors employed, the more robust the authentication system.[8] In this regard, MFA may provide more robust authentication than two or one-factor methods of authentication.

- Properly implemented, MFA can offer one of the best defenses to password-related attacks and significantly decrease the risk of an account takeover.
    - Although the use of MFA can prevent bad actors from successfully logging into a customer's account or into a system to which a staff member has access, it cannot prevent bad actors from identifying which accounts are valid user accounts on the targeted website.
    - Identified accounts may become the targets of future attacks and information concerning the existence and validity of the accounts may be sold to other bad actors, who may attempt to pass the final MFA verification step through other means, such as phishing emails, online research of targeted individuals, and social engineering;
- <u>Completely Automated Public Turing test to tell Computers and Humans Apart ("CAPTCHA")</u>. To combat automated scripts or bots used in the such attacks, deployment of a CAPTCHA, which requires users to confirm they are not running automated scripts by performing an action to prove they are human (e.g., identifying pictures of a particular object within a grid of pictures or identifying words spoken against a background of other noise);
- <u>Controls to Detect and Prevent</u>.
    - Implementation of controls to detect and prevent credential stuffing attacks. This can include monitoring for a higher-than-usual number of login attempts over a given time period, or a higher-than-usual number of failed logins over a given time period.[9]
        - Firms then use tools to collect information about user devices and create a "fingerprint" for each incoming session. The fingerprint is a combination of parameters such as operating system, language, browser, time zone, user agent, etc. For example, if the same combination of parameters logged in several times in rapid sequence, it is more likely to be a brute force or credential stuffing attack;
    - Use of a Web Application Firewall ("WAF") that can detect and inhibit credential stuffing attacks;

[8] *See* NIST SP 800-63-3, supra note 6.

[9] For example, some firms have implemented account monitoring controls to identify and escalate anomalous activity.

  - Offering or enabling additional controls that can prevent damage in the event an account is taken over, such as controls over, or limiting online access to, fund transfers and accessing PII; and,

- Monitoring the Dark Web. Surveillance of the dark web for lists of leaked user IDs and passwords, and performance of tests to evaluate whether current user accounts are susceptible to credential stuffing attacks.

IV. Other Considerations in Preparing for Credential Stuffing Attacks

As firms prepare for credential stuffing attacks, OCIE staff encourages firms to consider their current practices (e.g., MFA and other practices described above) and any potential limitations of those practices, and to consider whether the firm's customers and staff are properly informed on how they can better secure their accounts.

Informed Customers

Most firms require customers and staff to create and use strong passwords. However, the use of passwords is less effective if customers and/or staff re-use passwords from other sites. To be more effective, some firms have informed and encouraged clients and staff to create strong, unique passwords and to change passwords if there are indications that their password has been compromised.[10]

Firm Defenses: Multi-Factor Authentication and the Use of Mobile Phones

Mobile phone text messages are often used as a verification method for MFA but this method is not foolproof. Mobile phone text messages rely on the use of proper security by mobile phone providers to authenticate account holders properly when transferring phone numbers between devices. Some firms highlight for account owners and staff that they should be alert to instances where their mobile devices no longer work, as someone may have attempted fraudulently to transfer their phone number to another device.

V. Conclusion

Financial institutions should remain vigilant and proactively address emergent cyber risks. OCIE encourages firms to review their customer account protection safeguards and identity theft prevention programs and consider whether updates to such programs or policies are warranted to address emergent risks. In addition, firms are encouraged to consider outreach to their customers to inform them of actions they may take to protect their financial accounts and personally identifiable information.

[10] Recent NIST password guidelines note that password changes are not required unless there is evidence that an account has been compromised. *See e.g.*, NIST Special Publication 800-63-B, Digital Identity Guidelines: Authentication and Lifecycle Management, available at https://pages.nist.gov/800-63-3/sp800-63b.html.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.