OCIE Provides Cybersecurity Risk Alert to Investment Advisers and Broker-Dealers Regarding Credential Stuffing

September 24, 2020

AUTHORS

Elizabeth P. Gray | Richard M. Borden | Daniel K. Alvarez | Elizabeth Bower
Marc J. Lederer

The SEC's Office of Compliance Inspections and Examinations ("OCIE") warned in a cybersecurity risk alert ("Risk Alert") on September 15, 2020 that it has observed in recent examinations an increase in the number of cyber attacks using a tactic called "credential stuffing" against SEC-registered investment advisers and brokers and dealers ("SEC Registrants").[1] The Risk Alert highlights a number of practices that SEC Registrants have taken in response to these attacks, the details of which are described below. The Risk Alert encourages registrants to consider reviewing and updating their Regulation S-P and Regulation S-ID policies and programs to address the growing risk of credential stuffing.

In a credential stuffing attack, the attacker uses credentials (user names, email addresses, passwords and other related information) compromised in prior breaches to test the compromised user names and passwords on websites of financial firms, often using automated scripts that allow the attackers to test hundreds or thousands of credentials in seconds. As many consumers use the same user names and passwords across multiple websites, these attacks are effective far too often. Attackers that gain access to the accounts then steal assets, access more customer confidential information (including personally identifiable information), obtain additional login credentials that they can sell to other bad actors, and even take over the customer accounts. OCIE observed that Internet-facing systems and third-party systems are particularly vulnerable to these attacks. OCIE stated that "[t]he failure to mitigate the risks of credential stuffing proactively

[1] Text of OCIE Risk Alert, "Cybersecurity: Safeguarding Client Accounts against Credential Compromise," available here.

significantly increases various risks for firms, including but not limited to financial, regulatory, legal, and reputational risks, as well as, importantly, risks to investors."

In the Risk Alert, OCIE identified the following practices from SEC Registrants in response to credential stuffing:

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

- Multi-Factor Authentication ("MFA"). Use of MFA, which employs multiple "verification methods" to authenticate the person seeking to log into an account. According to OCIE, MFA can offer one of the best defenses to password-related attacks and significantly decreases the risk of an account compromise and takeover.[2]

- Completely Automated Public Turing Test To Tell Computers and Humans Apart ("CAPTCHA"). To combat automated scripts or bots used in 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).

- Controls to Detect and Prevent. Implementation of controls to detect and prevent credential stuffing attacks, including:

- 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;

- Creating a "Fingerprint" of each incoming session, e.g., a log of different parameters, such as operating system, language, browser, time zone, user agent, etc., that would allow the system to determine whether the traffic is from the same origin;

- Use of a Web Application Firewall ("WAF") that can detect and inhibit credential stuffing attacks; and

- 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 personally identifiable information.

[2] OCIE further noted that even though MFA is an effective defense, the use of MFA cannot prevent bad actors from identifying which accounts are valid user accounts on the targeted website and those accounts may become the targets of future attacks. Identified 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.

- 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. Such monitoring has risk in and of itself, and needs to be conducted deliberately and according to appropriate legal steps.

OCIE encourages SEC Registrants to also inform their customers about how to better secure their accounts in light of these attacks. According to OCIE, informing customers should include a discussion of the use of strong, unique passwords that are not reused across multiple sites.

Other agencies have also taken notice of the dangers of credential stuffing. FINRA (the Financial Industry Regulatory Authority) has published a cybersecurity alert on these types of attacks[3] and a recent FBI report stated that the majority of security incidents against financial institutions between 2017 and 2020 were the result of credential stuffing and distributed denial of service attacks.[4]

While a number of SEC Registrants may already be requiring the use of strong passwords and MFA, this Risk Alert highlights the importance of credential updating policies. SEC Registrants may also want to consider whether to use other security practices, such as CAPTCHA and enhanced monitoring and controls, to help combat cyber attacks such as credential stuffing. SEC Registrants should review their cybersecurity programs with an eye toward improving their maturity level and overall control environment.

[3] Text of FINRA "Cybersecurity Alert: Cloud-Based Email Account Takeovers," available here.

[4] Text of FBI Report, "Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector," available here.

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters, and CFTC and bank regulation. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Marc J. Lederer
212 728 8624
mlederer@willkie.com