KILPATRICK TOWNSEND

October 14, 2020

OCIE Issues Second Cybersecurity Risk Alert of Q3-2020

by Jeffrey T. Skinner , Lauren C. Jackson , Michael MacRae Robinson

---

On September 15, 2020, the SEC's Office of Compliance Inspections and Examinations (" *OCIE*") issued a cybersecurity risk alert highlighting the increased use of "credential stuffing" attacks against investment advisers and broker dealers. (In July, OCIE issued a cybersecurity risk alert regarding ransomware.)

Credential stuffing is an automated attack on web-based user accounts and network login account credentials. Cyber attackers obtain lists of usernames, email addresses, and corresponding passwords from a variety of sources, including the dark web, and then employ automated scripts to try to gain access to customer accounts. When a credential stuffing attack succeeds, the cyber attackers are able to gain access to confidential customer information, which they can then sell to other bad actors or use to steal assets from customers.

OCIE observed that successful credential stuffing attacks occur more often when: (1) individuals use the same password or minor variations of the same password for various online accounts; and (2) individuals use login usernames that are easily guessed such as email addresses or full names.

While credential stuffing is far more effective than traditional brute force attacks, OCIE observed a variety of measures that help to protect client accounts, including:

1. Periodic review of policies and programs with specific focus on updating password policies to incorporate a recognized password standard requiring strength, length, type, and change of passwords;
2. Implementation of controls to detect and prevent credential stuffing attacks such as monitoring for a high-than-usual number of failed logins over a given time period and use of a web application firewall;
3. Use of multi-factor authentication, which employs multiple verification methods to authenticate the person seeking to log in to an account (e.g., requiring entry of a verification code sent to a known-cell phone number to access the account by computer);
4. To combat automated scripts or bot attacks, use of Completely Automated Public Turing Test to Tell Computers and Humans Apart (i.e., "CAPTCHA"), which requires users to confirm they are not running automated scripts by performing an action to prove they are human (e.g., checking the "I am not a robot" box, and then identifying pictures of a particular object); and
5. Monitoring the dark web for lists of leaked user identifications and passwords, and performance tests to

evaluate whether current user accounts are susceptible to credential stuffing attacks.

The failure to mitigate the risk of credential stuffing attacks causes increased risks to firms, including reputational, regulatory, legal, and financial risks. In order to address emerging cyber security risks, it is critical that firms remain vigilant by periodically reviewing their policies and procedures and employing preventative controls such as multi-factor authentication. We also encourage investment advisers and broker dealers to reach out to their clients to inform them of actions they can take to safeguard their accounts and personally identifiable information. In addition to the SEC, states also have robust cybersecurity requirements for investment advisers and broker dealers.

If you have any questions about measures that investment advisers or broker dealers can and should take to reduce the risks that cybersecurity attacks pose and to otherwise comply with regulatory cybersecurity requirements, please feel free to contact us.

By the ***Investment Management and Broker-Dealer Team*** at Kilpatrick Townsend & Stockton