Debevoise
& Plimpton

Debevoise Update D&P

It’s Time to Take Credential Stuffing Seriously

September 30, 2020

We have recently written about the persistence of the three most common cyber attacks: Ransomware, Phishing and Business Email Compromises (BECs) and the increased regulatory scrutiny that companies face when they fall victim to these attacks. Two recent developments demonstrate that credential stuffing is yet another serious cybersecurity risk that is on the rise and has the attention of regulators. First, on September 15, 2020, New York’s Attorney General, Letitia James, announced a $650,000 settlement with Dunkin’ Donuts, stemming from a 2015 security breach that targeted almost 20,000 customers using credential stuffing. Second, on the same day, the Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (“OCIE”) issued a risk alert (the “Risk Alert”) on observed best practices by registered investment advisers and broker-dealers (together, “firms”) to protect customer accounts against credential stuffing. In this client update, we will discuss the cybersecurity and regulatory risks posed by credential stuffing and several ways to mitigate these risks.

What is Credential Stuffing? As more of our activities move online, the number of passwords we require increases. In order to be able to remember them all, most people use the same username/password combination for multiple online accounts or use very similar passwords (e.g., changing one number). The result is that all of the accounts that use the same login credentials are vulnerable if any one of them is compromised because attackers can use automated tools to take stolen usernames/passwords from one account and website and test to see if those same credentials (or very similar credentials) work for other accounts and websites. Threat actors acquire the credentials that they use for these attacks through their own phishing and hacking activities, or by purchasing bulk credentials stolen by others, which are available on the dark web. As more companies fall victim to data breaches, the pool of compromised credentials that can be used for these attacks gets bigger, and thereby the overall risk increases.

Like phishing, credential stuffing is often not an attack by itself but a means to gain access to an online account to launch another attack (e.g., load ransomware, send phishing emails, make purchases using the compromised account, transfer funds to the attackers’ account, exfiltrate confidential personal or company data, etc.).

The Dunkin' Case. In September 2019, the New York Attorney General filed a suit against Dunkin' Brands, Inc. (the franchisor of Dunkin' Donuts). The Complaint alleged failures of Dunkin' to undertake appropriate actions to investigate, notify and remediate in the aftermath of a series of credential stuffing attacks that allowed criminals to gain access to 10s of thousands of Dunkin's customer accounts. The attackers made purchases using the customers' DD cards and also sold those DD cards online.

In addition to the payment, the settlement requires Dunkin' to provide refunds for unauthorized use of DD cards. Dunkin' must also maintain safeguards to protect against similar attacks in the future and follow incident response procedures when an attack occurs.

According to the AG's press release, Dunkin' was repeatedly alerted to attackers' ongoing attempts to log in to customer accounts, but Dunkin' failed to (i) conduct an investigation into the attacks, (ii) identify other customer accounts that had been compromised, (iii) determine what customer information had been acquired or funds had been stolen, (iv) protect the nearly 20,000 customers that it knew had been impacted in the attacks, (v) reset the account passwords to prevent further unauthorized access and (vi) freeze the compromised DD cards.

It is important to note this case arose before the New York SHIELD Act came into effect and so was brought under the state's general consumer protection laws—not focusing directly on substantive shortfalls in cybersecurity but alleging that Dunkin deceived consumers by making misrepresentations about the security of their personal information. All states have similar powers to take enforcement action against deceptive practices, as does the FTC. There is also an "unfairness" prong to these consumer protection statutes, which regulators have sometimes relied on to allege substantive security shortcomings. The FTC has also relied on the Privacy Rule and the Safeguards Rule of the Gramm–Leach–Bliley Act to bring an enforcement action for failing to take steps to prevent credential stuffing.

Credential Stuffing and Breach Notification. An additional claim by the AG was that Dunkin' violated New York's breach notification laws by failing to alert affected customers. Companies have questioned whether a credential stuffing attack is really "their" breach for notification purposes when the misused credentials were stolen from another company in a prior incident. Whether a successful credential stuffing attack triggers breach notification obligations is a complicated question. Some state laws treat login credentials themselves as personal data, and if the credentials are used to log in to the client's system, that may trigger notification obligations, depending on the state and what data was accessed from the account. Similar issues arise under the GDPR where it is at least questionable whether a successful credential stuffing attack, in and of itself, always involves a "breach of security" sufficient to potentially trigger notification.

For federal and state laws in the U.S., Debevoise has developed a tool to help companies quickly assess their breach notification obligations. Clients who are interested in joining the small group of companies that are beta testing the Debevoise Data Portal, please contact us at dataportal@debevoise.com for more information.

Ways to Reduce Risk of Credential Stuffing. The AG's press release in the Dunkin' case notes that New York's safeguards law—General Business Law § 899-bb—requires that businesses maintain reasonable safeguards to protect New York residents' private information and that these safeguards should include appropriate measures to mitigate risks associated with credential stuffing including:

- Conducting a reasonable investigation to identify customers impacted in a credential stuffing attack; and
- Taking appropriate action to protect those impacted customers such as resetting customers' passwords, freezing customers' accounts or alerting customers to a compromised account.

In its Risk Alert, OCIE observed an increase in credential stuffing attacks against registrants. OCIE emphasized that firms should remain vigilant and proactive in their efforts, and it encouraged firms to consider their current practices and systems, review their policies and programs and make any necessary updates taking into account the observed best practices highlighted below.

Periodic Review of Password Requirements: OCIE recommends that firms periodically review and update their password requirements to ensure that both customer and employee passwords are consistent with industry standards for strength, length, type and frequency of changing passwords.

Multifactor Authentication ("MFA"): MFA involves using more than one verification method to authenticate the person seeking to log in to an account such as requiring (in addition to a username and password) a code that is sent by email or text to a verified email address or phone number. The code can also be obtained through an app such as RSA SecureID, Duo or Google Authenticator. MFA does not, however, resolve all credential stuffing risks. Customers often do not alert firms of changes in their second factor email address or phone number. In addition, MFA may be more suitable for remote access to employee accounts than customer accounts given the additional time it can add to the log-in process. To reduce this friction, firms may instead consider using a modified MFA, where the second factor is only required when a user logs in from a new device or fails more than one log-in attempt. Similarly, MFA can be enabled for only certain accounts (e.g., funds transfers, upgrading subscription services, etc.) or for entering areas of accounts that may disclose individuals' personal information.

Finally, while not possible in many cases, those wanting to go even further could consider moving towards a "passwordless" authentication model, relying on a "possession factor" (e.g., an email address, telephone number, device etc. known to be associated with a specific individual) or an "inherent factor" (typically biometrics such as voice signature). While passwordless models create new challenges (e.g., legal requirements for the collection and use of biometric data), they can significantly reduce the risk of credential stuffing risk in the right circumstances.

Completely Automated Public Turing test to tell Computers and Humans Apart ("CAPTCHA"): To combat automated scripts used in credential stuffing attacks, OCIE observed the use of some form of CAPTCHA, which requires users to perform a task that is relatively easy for humans, but is hard for bots (e.g., identifying a particular object within a grid of pictures, or wavy letters that appear against a background of noise). This too is often limited to situations where customers log in from a new device or enter an incorrect password more than once. With CAPTCHA solutions becoming more advanced as time goes on, companies may want to periodically review whether the their CAPTCHA solution remains in step with market practice and is configured to operate in a way proportionate to the company's risk of credential stuffing. That said, even the most sophisticated CAPTCHA solutions can struggle to tackle the risk of crowd sourced CAPTCHA puzzle solving where attackers pay humans to solve them and help attackers fly under the radar.

Technical Login Controls: These include monitoring for a higher-than-usual number of log-in attempts over a given time period, freezing account access after a certain number of unsuccessful log-in attempts and use of Web Application Firewalls that can detect and inhibit credential stuffing attacks. Other measures include controls that prevent damage in the event an account is taken over such as access controls and the need for additional authentications for funds transfers.

Dark Web Monitoring and Password Testing: This involves hiring a vendor to search the dark web for lists of leaked user IDs and passwords and perform tests to see whether current user accounts are susceptible to credential stuffing attacks. Additionally, companies can use lists of commonly breached passwords to create password "blacklists" to prevent weak passwords being used.

Conclusion. Credential stuffing attacks are not new, but unfortunately (like phishing, ransomware and BECs), they are becoming more sophisticated and resulting in more damage. Regulators recognize these developments, and they expect firms and companies alike to "own" these attacks and fight back hard. Using more of the tools at their disposal, regulators seem increasingly ready to hold companies and firms accountable for not effectively combating credential stuffing.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Norma Angelica Freeland
nafreeland@debevoise.com

WASHINGTON, D.C.

Marc Ponchione
mponchione@debevoise.com

Gregory T. Larkin
gtlarkin@debevoise.com

LONDON

Robert Maddox
rmaddox@debevoise.com