Credential Stuffing: Cyber Best Practices from NY Attorney General's Latest Report

Alysa Z. Hutnik, Paul L. Singer, Laura Riposo VanDruff, Beth Bolen Chun, Alexander I. Schneider

January 13, 2022

In guidance released last week, the New York State Office of the Attorney General urged businesses to incorporate safeguards to detect and prevent credential-stuffing attacks in their data security programs. The guidance stemmed from the AG's finding that 1.1 million customer accounts at "well-known" companies appeared to have been compromised in credential-stuffing attacks.

Credential stuffing refers to an attack where a hacker uses stolen usernames and passwords, or "credentials," from an online service that has suffered a data breach to access other online services, according to the AG's report. Attackers exploit the habit of some consumers to reuse their passwords across multiple websites. Attackers may also use automated software to initiate login attempts using stolen credentials from the dark web.

"Businesses have the responsibility to take appropriate action to protect their customers' online accounts and this guide lays out critical safeguards companies can use in the fight against credential stuffing," New York State Attorney General Letitia James wrote in a press release accompanying the report.

Specifically, the AG report states that data security programs should incorporate safeguards against the threat of credential stuffing in four areas: (1) defending against credential-stuffing attacks, (2) detecting a credential stuffing breach, (3) preventing fraud and misuse of customer information, and (4) responding to a credential stuffing incident.

The AG recommends that businesses implement the following safeguards to mitigate the risk of successful credential-stuffing attacks. Which safeguards are appropriate to a business will depend on the size and complexity of the business, the volume and sensitivity of customer information it maintains, the risk and scale of injury, and the software and systems already in use.

Defend against a credential-stuffing attack

- **Bot Detection –** Businesses can leverage bot detection software to distinguish automated log in attempts from regular "human" log in attempts, and to block malicious bots. The AG noted, however, that in its view CAPTCHA systems have been less effective than bot detection software.
- **Multi-Factor Authentication –** Multi-factor authentication creates an additional hurdle to logging in to an account by requiring users to not only have appropriate credentials but also a device that issues authentication codes or biometric authentication procedures.

- **Passwordless Authentication –** Passwordless authentication allows a user to access their account using an authentication procedure, such as a one-time code or emailed link.
- **Web Application Firewalls (WAF) –** WAFs that guard against malicious traffic can also include safeguards that protect against credential stuffing. These safeguards include rate limiting, which blocks or throttles repeated log in attempts; HTTP request analysis, which analyzes header information and other metadata for indicators of malicious traffic; and IP address blacklists, which block IP addresses known to have engaged in attacks.
- **Preventing Reuse of Compromised Passwords –** Businesses can implement procedures to prevent customers from reusing passwords that have been previously compromised, using vendors that compile such credentials.

Detecting a Credential Stuffing Breach

- **Monitoring Customer Activity –** Businesses may monitor indicators of fraudulent activity to protect customer accounts.
- **Monitoring Customer Reports of Fraud –** Businesses may also review reports from customers about unauthorized transactions or account access.
- **Notice of Account Activity –** Businesses may notify customers of unusual account activity to help the customer identify unauthorized activity and report it to the business.
- **Threat Intelligence –** Businesses may utilize threat intelligence firms that monitor dark web activity for discussion of stolen credentials or accounts.

Preventing Fraud and Misuse of Customer Information

- **Re-authentication at the Time of Purchase** – To prevent attackers from leveraging stolen accounts to make a purchase, the AG states that businesses may require users to re-authenticate stored payment information. For example, the user may be required to re-enter their credit card number or CVV code, or the company might send the user an authentication code.
- **Third Party Fraud Detection –** Companies may use third-party services that identify suspicious or fraudulent transactions.
- **Mitigating Social Engineering –** Anticipating that some hackers may try to convince customer service personnel to authenticate their account, companies can develop policies that anticipate social engineering attacks and train relevant personnel on those attacks.
- **Preventing Gift Card Theft –** The AG suggests that transferring gift cards between customer accounts and transferring funds between gift cards should be restricted or require re-authentication; and that companies should only display the last four digits of a gift card number.

Incident Response

- **Investigation –** Where companies suspect an attack, the new guidance states that companies should conduct a timely investigation to determine, at a minimum, “whether customer accounts were accessed without authorization, and, if so, which accounts were impacted, and how attackers were able to bypass existing safeguards.”

- **Remediation –** Companies should take action to remediate credential-stuffing attacks, according to the AG's guidance. The AG suggests blocking attackers' continued access to the accounts, resetting passwords, and freezing relevant accounts, where appropriate.
- **Notifying Customers –** The AG states that businesses should "quickly notify each customer whose account has been, or is reasonably likely to have been, accessed without authorization." The AG's report states that customer notice should include the following elements:
    - Disclosing whether the particular customer's account was accessed without authorization;
    - The timing of the attack;
    - What customer information was accessed; and
    - What actions have been taken to protect the customer.

Finally, given the evolving nature of credential stuffing-related threats, the AG warns that businesses should continually evaluate the effectiveness of applicable controls and implement new procedures where appropriate.

* * *

Since State AGs don't typically issue guidance like this, it may be a sign that New York plans to continue to target businesses who have not followed their guidance and have thus allegedly inadequately protected against credential stuffing. While other states aren't bound by this NY-specific guidance, other State AG offices are likely to take notice and discuss this unusual measure through their standing working groups. As a result, some states may potentially follow suit and launch their own investigations on credential stuffing.

State and federal regulators are active in this space, investigating companies' compliance with UDAP, FTCA, and FCRA Red Flags. Including the possibility of credential stuffing in your data security risk assessment and policy review may reduce your regulatory exposure.

Please join us for **Privacy Priorities for 2022: Legal and Tech Developments to Track and Tackle**, a joint webinar between Kelley Drye's Privacy Team and Ketch, a data control and programmatic privacy platform. This Data Privacy Week webinar will highlight key legal and self-regulatory developments to monitor, along with practical considerations for how to tackle these changes over the course of the year. This will be the first in a series of practical privacy webinars by Kelley Drye to help you keep up with key developments, ask questions, and suggest topics that you would like to see covered in greater depth. Register here.

Also please join us for **State Attorney General Consumer Protection Priorities for 2022**. This webinar will provide discussion and practical information on the topics mentioned above and other state consumer protection, advertising, and privacy enforcement trends. Register here.