Published on *The National Law Review* https://natlawreview.com

# Preventing “Credential Stuffing” Attacks, Guidance from NY State Attorney General Letitia James

Article By:

Joseph J. Lazzarotti

After reading New York Attorney General Letitia James’ Business Guide for Credential Stuffing Attacks (“Guide”), I promptly reminded my family (and myself!) to change passwords. The practice of using the same password for multiple online accounts is one that most, if not all of us, use from time to time. According to a recent study, the average person has 100 passwords to remember! While individuals can be more personally responsible about their password management, there is a growing emphasis on what organizations can be doing. That is the focus of AG James’ report.

It is unclear whether or to what extent the New York Attorney General’s office will be increasing its investigation and/or enforcement of incidents involving credential stuffing. However, organizations should be reminded of the New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) that fully went into effect March 21, 2020. In short, the SHIELD Act requires businesses to adopt reasonable safeguards to protect personal information of New York residents. The law empowers the AG to obtain civil penalties. For knowing and reckless violations, a court may impose penalties of the greater of $5,000 or up to $20 per instance with a cap of $250,000. For reasonable safeguard requirement violations, a court may impose penalties of not more than $5,000 per violation. For more information on the SHIELD Act, please see our FAQs.

## What is “credential stuffing”?

Cyber criminals know we juggle many passwords. They also know we juggle a lot of other things as well and may not have the best cyber hygiene – we use the same credentials across multiple online accounts to make remembering easier. So, they engage in “credential stuffing.” This form of cyberattack typically involves repeated attempts to log in to online accounts using usernames and passwords stolen from other online services. So, when you hear news reports about a data breach involving the exfiltration of online account credentials belonging to thousands or millions of users, it is that information, as one example, that is used in these attacks on other accounts.

## What do attackers do when successful at credential stuffing?

The attackers fail in their efforts more than they succeed. They work to improve their odds typically by leveraging readily available software to quickly send hundreds of thousands of login attempts without human intervention.

When they are successful, they can gain access to very sensitive information maintained in the account, including the account holder's name, address, purchase history, payments information, the name and addresses of other individuals connected to the account holder, etc. As the Guide explains, with that access, the attackers can, for example:

> ***make fraudulent purchases using the customer's saved credit card, steal and sell a gift card that the customer has saved on the account, use customer data stolen from the account in a phishing attack, or simply sell the login credentials to another individual on the dark web.***

## Why is the NY Attorney General concerned about "credential stuffing"?

Recognizing that credential stuffing attacks have resulted in a significant cost to businesses and consumers, Office of the New York State Attorney General (OAG) launched an investigation to better understand the impact of credential stuffing. During the investigation, the OAG monitored online communities dedicated to credential stuffing and found thousands of posts containing valid login credentials. Members of these communities were free to use these valid credentials to break into the customer accounts themselves, or use them for their own credential stuffing attacks on other companies' websites and apps.

> ***After reviewing thousands of posts, the OAG compiled login credentials for customer accounts at 17 well-known companies, which included online retailers, restaurant chains, and food delivery services. In all, the OAG collected credentials for more than 1.1 million customer accounts, all of which appeared to have been compromised in credential stuffing attacks.***

In the course of the investigation and working with the companies to address the findings, the OAG was able to review and evaluate the effectiveness of a wide range of safeguards against credential stuffing. It compiled a nonexhaustive list of those safeguards in the Guide, recognizing that not every safeguard is appropriate for every business. However, the OAG recommends that every business should maintain effective safeguards for defending against unauthorized access to customer accounts through credential stuffing attacks.

## What should organizations do to prevent credential stuffing?

First, it is important to recognize this is not just a concern for "businesses" or for-profit entities like the group of entities the OAG identified above. Many, if not most, organizations with an online presence use an online account or similar means to stay in touch with their customers, students, members, donors, employees, or other constituents. It is entirely possible for an individual to use the same username and password for accounts maintained with their favorite charity, their online email account, a local restaurant, and their Amazon Prime account. Of course, as suggested above, this practice should be avoided!

When organizations set out to prevent credential stuffing, they should evaluate which safeguards to implement in the context of their own operations, considering factors like (i) the size and complexity of the organization, (ii) the volume and sensitivity of personal information that it maintains, (iii) the risk and scale of injury should that information be compromised, and (iv) the software and systems that are already in use. These are similar to factors we see repeatedly when applying many data security frameworks.

The OAG reminds organizations that the effectiveness of the safeguards available to prevent credential stuffing will likely change over time as attackers adopt new tactics. So, organizations need to continue to be vigilant and update their approaches as these changes occur.

For organizations that maintain online accounts, the Guide calls for them to adopt a data security program with effective safeguards in four areas:

1. Defending against credential stuffing attacks, with safeguards such as:
    - Bot detection
    - Multifactor authentication
    - Passwordless authentication
2. Detecting a credential stuffing breach, with safeguards such as:
    - Monitoring user activity
    - Promptly addressing reports of fraud
3. Preventing fraud and misuse of customer information, with safeguards such as:
    - Reauthentication at point of purchase
    - Third party fraud detection
    - Mitigating social engineering
4. Responding to a credential stuffing incident:
    - Investigation
    - Remediation
    - Notification

Several of these safeguards should look familiar to organizations that have been developing and/or maintaining information security policies and procedures. However, the Guide goes into more detail on each one, providing a helpful roadmap and their relation to credential stuffing. Of course, as noted, organizations should evaluate which of these are appropriate considering their particular circumstances. It also is worth noting that many of these safeguards can have benefits beyond credential stuffing prevention.

National Law Review, Volume XII, Number 10

Source URL:https://natlawreview.com/article/preventing-credential-stuffing-attacks-guidance-ny-state-attorney-general-letitia