Office of the New York State
Attorney General Letitia James

Bureau of Internet and Technology

Business Guide for Credential Stuffing Attacks

January 5, 2022

Introduction

Virtually every website and app uses passwords as a means of authenticating its users. Users — forced to contend with an ever-expanding number of online accounts they must manage — tend to reuse the same passwords across multiple online services. Unfortunately, the widespread use and reuse of passwords has made them attractive targets to cybercriminals, who know that passwords stolen from one company may provide the keys to a host of accounts at another.

According to a recent study, there are more than 15 billion stolen credentials circulating on the Internet.[1] This enormous cache of credentials has fueled a dramatic rise in credential stuffing attacks. The operator of one large content delivery network reported that it witnessed more than 193 billion such attacks in 2020.[2]

These attacks are extraordinarily costly for both businesses and consumers. The Ponemon Institute's Cost of Credential Stuffing report found that businesses lose an average of $6 million per year to credential stuffing in the form of application downtime, lost customers, and increased IT costs.[3]

In light of this growing threat, the Office of the New York State Attorney General (OAG) launched an investigation to identify businesses and consumers impacted by credential stuffing. Over the course of this investigation, the OAG was able to review and evaluate the effectiveness of a wide range of safeguards against credential stuffing. The purpose of this document is to share some of the lessons learned, including concrete guidance to businesses on steps they can, and should, take to better protect against credential stuffing attacks.[4]

[1] Digital Shadows, From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover (2020), https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover

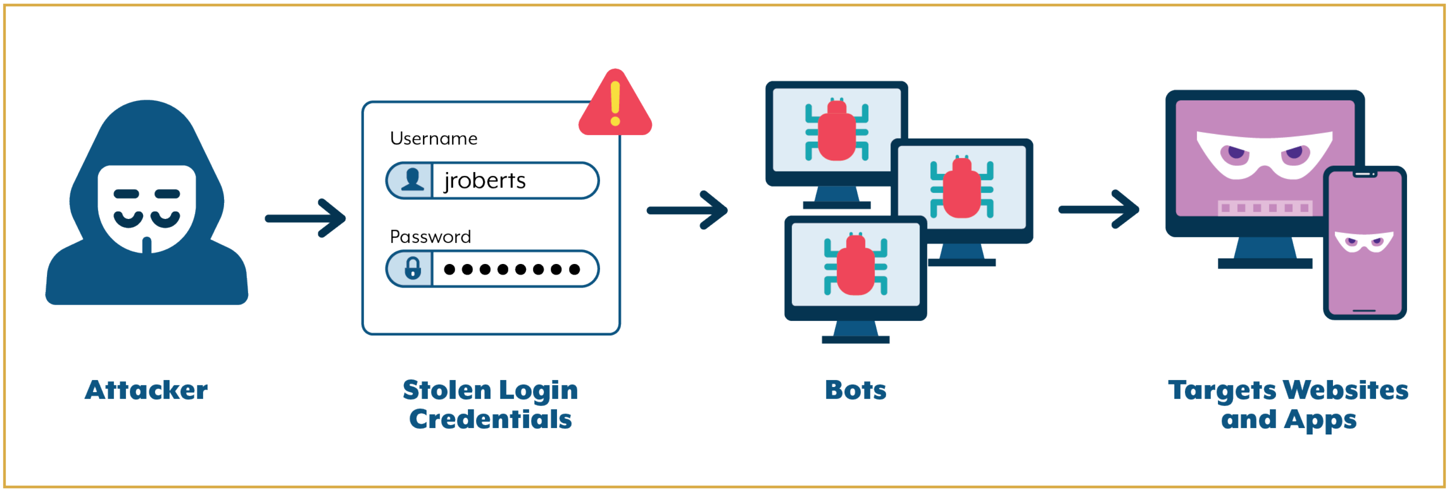
[2] Akamai, Phishing for Finance (May 2021), https://www.akamai.com/content/dam/site/en/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf

[3] Ponemon Institute, The Cost of Credential Stuffing (2017), https://www.akamai.com/lp/report/ponemon-the-cost-of-credential-stuffing-report

[4] This guide is not intended to supersede existing federal or state laws or regulations concerning data security.

A. What is Credential Stuffing?

Credential stuffing is a type of cyberattack that typically involves repeated attempts to log in to online accounts using usernames and passwords stolen from other online services. It leverages the natural human tendency to reuse passwords to cope with the ever-growing number of online accounts that must be managed. Attackers know that the username and password used at one website may also be used at a half-dozen others.

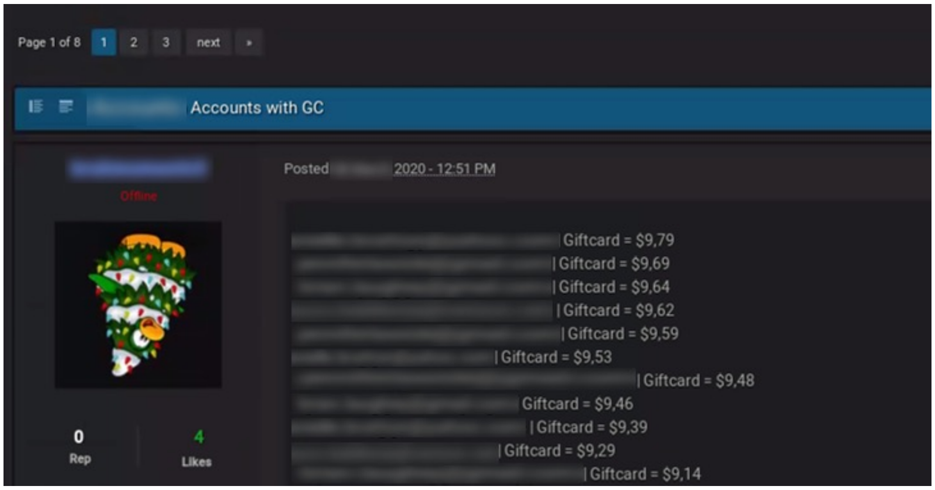


Unlike many other types of cyberattacks, credential stuffing attacks often require little technical knowledge to mount. Attackers typically use free, easily accessible software capable of transmitting hundreds of login attempts simultaneously without human intervention. A single attacker can easily send hundreds of thousands, or even millions, of login attempts to a single web service.

Although most login attempts in a credential stuffing attack will fail, a single attack can nevertheless yield thousands of compromised accounts due to the sheer volume of attempts. Attackers have a variety of ways of monetizing these compromised accounts. They 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.

B. Our Investigation

Over a period of several months, the OAG monitored several online communities dedicated to credential stuffing. The OAG found thousands of posts containing login credentials that had been tested in credential stuffing attacks on a website or app and confirmed to provide access to a customer account. Members of these communities were free to use these validated credentials to break into the customer accounts themselves, or use them for their own credential stuffing attacks on other companies' websites and apps.



[redacted] Accounts with GC

[redacted]

Posted [redacted] 2020 - 12:51 PM

[redacted] | Giftcard = $9,79
[redacted] | Giftcard = $9,69
[redacted] | Giftcard = $9,64
[redacted] | Giftcard = $9,62
[redacted] | Giftcard = $9,59
[redacted] | Giftcard = $9,53
[redacted] | Giftcard = $9,48
[redacted] Giftcard = $9,46
[redacted] | Giftcard = $9,39
[redacted] | Giftcard = $9,29
[redacted] | Giftcard = $9,14

Screenshot of post sharing validated customer account credentials

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.

The OAG contacted each of the 17 companies to alert them to the compromised accounts. The OAG also asked the companies to investigate and take steps to protect impacted customers. Every company did so.

The OAG also worked with the companies to determine how attackers had circumvented existing safeguards, and advised companies on steps they could take to enhance their data security programs and better secure customer accounts against credential stuffing. Over the course of the OAG's investigation, nearly all of the companies introduced, or presented plans to introduce, additional safeguards.

Protecting Customers from Credential Stuffing Attacks

Credential stuffing attacks have become so prevalent that they are, for most businesses, unavoidable. Every business that maintains online accounts for its customers should therefore have a data security program that includes effective safeguards for protecting customers from credential stuffing attacks in each of 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.

In the sections below, the OAG presents specific safeguards that have been found to be effective in each of these areas. The list is not exhaustive, but rather highlights safeguards that may be applicable to a broad range of businesses. However, not every safeguard will be appropriate for every business. Businesses should evaluate which safeguards to implement in the context of their own operations, considering factors like the size and complexity of the business, the volume and sensitivity of customer information that it maintains, the risk and scale of injury, and the software and systems that are already in use.

It is important to note that the effectiveness of the safeguards identified below will likely change over time as attackers adopt new tactics. Businesses should regularly evaluate the effectiveness of their own controls and implement new safeguards as appropriate.

A. Defending Against a Credential Stuffing Attack

Every business should maintain effective safeguards for defending against unauthorized access to customer accounts through credential stuffing attacks. For many businesses, this will require implementing an effective technical safeguard, like bot detection software or multi-factor authentication, as well as foundational safeguards, such as a web application firewall.

Most Effective Safeguards

1. Bot Detection

Credential stuffing attacks typically involve tens or hundreds of thousands of login attempts that have been generated by automated software, or “bots.” One of the most effective controls for mitigating this type of attack is a bot detection system — software specifically designed to identify and block bot-generated Internet traffic. Effective bot detection systems can distinguish between human and bot traffic even when the bot traffic has been disguised — for example, by rotating through multiple IP addresses or device identifiers.

Although bot detection systems can be developed in-house, many companies use third-party bot detection and mitigation services. One advantage of a third-party service is that it can operate across hundreds of websites and apps, providing access to a vast amount of data that can help reveal bot patterns that would not be apparent to a single website operator.

Bot detection can be highly effective at mitigating credential stuffing attacks. One restaurant chain reported to the OAG that its bot detection vendor had blocked more than 271 million login attempts over a 17-month period. Another company the OAG contacted saw more than 40 million login attempts blocked over a two-month period. Success stories like these have likely contributed to bot detection systems’ popularity — 12 of the companies the OAG contacted have implemented or have plans to implement a bot detection system.

CAPTCHA systems, which take a different approach to distinguishing between humans and bots, may not be as effective as other bot detection technologies. Software has become adept at solving many types of CAPTCHA challenges without human intervention. In addition, CAPTCHA challenges can be completed by actual humans in CAPTCHA farms, typically located overseas.

2. Multi-Factor Authentication

Another effective safeguard for preventing credential stuffing attacks is multi-factor authentication, also known as MFA. MFA requires a user to present two or more types of credentials in order to log in to their account. The credentials must come from two (or more) of the following categories:

1. Something the user knows (like a password),
2. Something the user has (like a mobile phone), and
3. Something the user is (like a fingerprint).

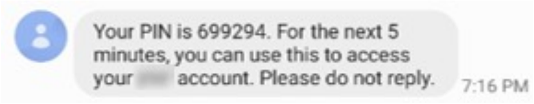
Most attackers that have access to a stolen password will not have access to other credential types.

Although MFA was historically used by organizations that maintained highly sensitive information, such as financial institutions, in recent years MFA has seen more widespread adoption. Six of the companies the OAG contacted use or have plans to implement MFA.

Companies often implement a second factor through one of three mechanisms:

1. A physical security key,
2. An authenticator app, or
3. Email or SMS text messages that contain a one-time code or link.

Physical security keys and authenticator apps are often more secure methods of authentication, as techniques like SIM swapping and social engineering can allow determined attackers to steal a code sent via text message or email. When selecting a mechanism to implement, businesses should weigh the risk of harm from an unauthorized login against the complexity and ease of use of the MFA system.



Your PIN is 699294. For the next 5 minutes, you can use this to access your [redacted] account. Please do not reply. 7:16 PM

Authentication code sent by SMS text message

Practice Tip

In a recent data breach investigation, the OAG uncovered evidence that more than 140,000 customer accounts had been compromised in credential stuffing attacks against a business that used multi-factor authentication. How had attackers bypassed MFA? They hadn't. The OAG found the MFA functionality had been implemented incorrectly, rendering it ineffective.

As with any safeguard, businesses should ensure their MFA implementation is both thoroughly tested and monitored for effectiveness.

3. Passwordless Authentication

Passwordless authentication is, as the name suggests, a method for authenticating users that does not rely on a password. Instead, users are authenticated using a different type of authentication factor, either “something the user has” or “something the user is.” Similar to MFA, most common implementations use an authenticator app, a one-time authentication code sent via SMS or email, or an emailed link.

Although passwordless authentication has not yet been widely adopted, it has gained traction in recent years. One of the companies the OAG contacted relies on passwordless authentication.

Other Safeguards

The safeguards listed below can also be helpful in mitigating credential stuffing attacks, but typically should be used in conjunction with other, more effective safeguards.

4. Web Application Firewalls

Most businesses should use a Web Application Firewall (WAF) as a first line of defense against malicious traffic. WAFs can include a variety of features capable of mitigating basic web application attacks. Sophisticated credential stuffing attacks, however, are often able to circumvent most WAF security measures. Several common WAF features are identified below.

Rate limiting: In most cases, businesses should block or throttle traffic from any user that has attempted to log in to multiple customer accounts in quick succession. This type of rate limiting is a low-cost control and can be effective against basic attacks.[5]

HTTP request analysis: Most WAFs analyze the header information and other metadata of incoming requests to identify traffic that is likely to be malicious. Businesses should consider implementing HTTP request analysis and evaluate whether blocking or throttling requests with the following characteristics would be effective in blocking malicious traffic:

- Requests that use IP addresses, or originate from networks, that have been identified as malicious.
- Requests that originate from a geographic area outside the customer base.
- Requests that originate from virtual private server providers such as Amazon Web Services or commercial data centers.
- Requests that originate from headless browsers, browsers that lack JavaScript execution engines, or have other attributes unique to common credential stuffing tools.

IP address blacklist: Some businesses maintain a list of IP addresses that have recently engaged in attacks, and block or throttle traffic associated with those IP addresses. Businesses can also subscribe to threat intelligence feeds offered by third parties to populate IP address blacklists.

5. Preventing Reuse of Compromised Passwords

Businesses can stop attackers from accessing at least some customer accounts by preventing customers from reusing passwords that have previously been compromised. This functionality typically relies on third-party vendors that compile credentials from known data breaches. When a customer selects a password, it is compared to the passwords in the library of stolen data; if the password matches, the customer is asked to choose another password.

[5] Attackers that disguise the source of a login attempt, for example by rotating through multiple proxy IP addresses, can often evade rate limiting controls.

B. Detecting a Credential Stuffing Breach

In the never-ending arms race against attackers, no safeguard is 100 percent effective. Every business should therefore have an effective means of detecting credential stuffing attacks that have bypassed other safeguards and compromised customer accounts. In most cases, this will require systematic monitoring of customer traffic. Other safeguards can supplement monitoring by providing a check using different sources of information.

Practice Tip

Several of the companies the OAG contacted had not detected the credential stuffing attacks that had compromised their customers' accounts.

Credential stuffing attacks are inevitable. If your business is not aware of credential stuffing attacks that have targeted your customers' accounts, chances are, your monitoring is inadequate.

Most Effective Safeguard

1. Monitoring Customer Activity

Most credential stuffing attacks can be identified through the footprints they leave on customer traffic. Attacks often appear as spikes in traffic volume or failed login attempts. Even sophisticated credential stuffing attacks have attack signatures that can be identified through analysis of customer activity. Most businesses should therefore have processes in place to systematically monitor customer traffic.

In most cases, monitoring should be at least partially automated to provide consistent, comparable metrics and round-the-clock surveillance. This automation might consist of a software process that runs in the background and alerts appropriate personnel if some benchmark is met; for example, when the number of failed login attempts over a certain period of time exceed a predefined threshold. In other cases, more sophisticated monitoring techniques will be appropriate.

WAFs and third-party bot detection services can provide effective monitoring capabilities as well as tools that can assist a business in reviewing customer traffic.

Other Safeguards

In most cases, the safeguards below will not be sufficient on their own to serve as an effective means of detecting successful attacks. However, they can be effective supplements to other security controls, like systematic monitoring.

2. Monitoring Customer Reports of Fraud

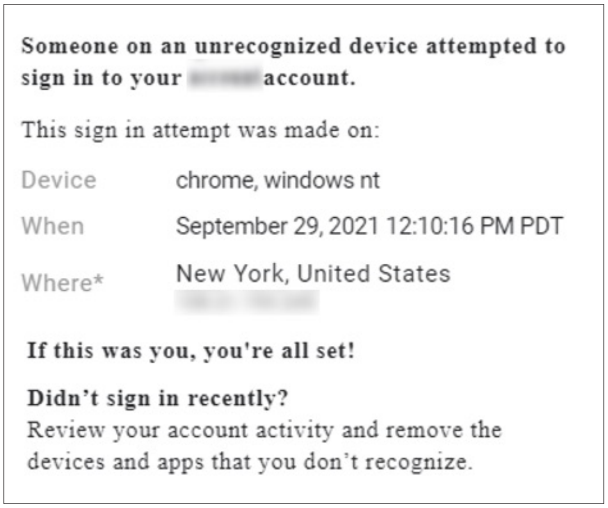
Customer reports of fraud and unauthorized access may indicate that customer accounts have been targeted in a credential stuffing attack. For example, attacks may be reflected in the volume of customer support inquiries a business receives. Patterns in what customers report — for example, repeated customer complaints of stolen gift card balances or unauthorized orders placed to an unrecognized address — can also indicate successful credential stuffing attacks.[6]

Businesses should consider systematically monitoring customer reports of fraud and unauthorized access for evidence of attacks. This might involve, for example, the regular review of fraud case volume over time to identify spikes or other patterns. Businesses should also set up clear channels of communication between customer service and information security personnel in order to detect and stop credential stuffing attacks as quickly as possible.

3. Notice of Account Activity

Notifying customers of unusual or significant account activity can serve several purposes. Notice provides the customer with an opportunity to review their account for unauthorized purchases or activity. If the customer determines the activity was unauthorized, they can report that unauthorized activity to the business. The business can then both take steps to protect the customer's account and use the report to help determine whether the unauthorized activity was part of a broader attack affecting other customers.

Businesses should identify appropriate triggers for sending notice. In many cases, a customer should be alerted when the customer's account has been accessed from an unrecognized device or a new location. In some cases, it may also be appropriate to notify customers when significant changes have been made to their accounts, such as a change in password or mailing address.



Someone on an unrecognized device attempted to sign in to your [redacted] account.

This sign in attempt was made on:

Device	chrome, windows nt
When	September 29, 2021 12:10:16 PM PDT
Where*	New York, United States [redacted]

If this was you, you're all set!

Didn't sign in recently?
Review your account activity and remove the devices and apps that you don't recognize.

Email notice of an account login using an unrecognized device

[6] A low volume of customer reported fraud is not a reliable indicator that credential stuffing has not occurred. Some attackers monetize compromised accounts without attracting customer notice.

4. Threat Intelligence

Following a successful attack, attackers will often share or sell customer account data they have stolen or customer login credentials they have validated. Many third-party threat intelligence firms offer services that monitor online messaging channels and forums for signs of a company's compromised credentials or accounts. Four of the companies the OAG contacted reported they used a threat intelligence company to monitor the Internet for signs that customer accounts have been compromised.

C. Preventing Fraud and Misuse of Customer Information

Every business should have effective safeguards in place for preventing an attacker with access to a customer account from making a fraudulent purchase using stored payment information or stealing customer funds.

Most Effective Safeguard

1. Re-authentication at the Time of Purchase

One of the most effective safeguards for preventing attackers from fraudulently using customers' stored payment information is re-authentication at the time of purchase. For certain payment methods, like credit cards, companies typically re-authenticate the stored payment information itself. For example, online merchants frequently require customers to re-enter the credit card number or CVV code when an order is placed to a new address using a stored credit card.

For other payment methods, including gift cards, store credit, and loyalty points, companies often re-authenticate the customer. For example, one restaurant chain sends its customers an authentication code when a customer uses loyalty points to place an order to a store location the customer has not previously visited. The customer must then enter the authentication code to complete the order.

Critically, businesses should require re-authentication for every method of payment they accept. The OAG encountered case after case in which attackers were able to exploit gaps in merchants' fraud protections by making a purchase using a payment method that did not require re-authentication.

Practice Tip

One tactic that attackers used at several of the companies the OAG contacted illustrates the importance of securing every method of payment.

At these companies, orders placed to a new address would require re-authentication if the customer paid using a stored credit card, but not if the customer used store credit. The OAG found that attackers that gained access to a customer account would initially place an order to an existing address using the customer's stored credit card. The attackers would then immediately cancel the order, obtain a refund in store credit, and place a new order to a new address using the just-issued store credit without completing any re-authorization.

Businesses should also identify appropriate triggers for re-authentication. As noted above, many merchants that ship or deliver goods require re-authentication when a customer enters a new address. However, this trigger will not be appropriate for all businesses and situations. For example, a chain restaurant that permits customers to pick up their meals may require re-authentication when an order is placed to a restaurant location the customer has not previously visited.

Other Safeguards

2. Third Party Fraud Detection

Some businesses use third-party services to identify suspicious or fraudulent transactions. These fraud detection services typically work by analyzing customer and transaction data for signs that a purchase is unauthorized. Although these services can identify and block certain fraudulent purchases, on their own they are generally not as effective at mitigating fraud as re-authentication based approaches. In addition, many of these services are only capable of analyzing credit card transactions and cannot be deployed with other payment methods.

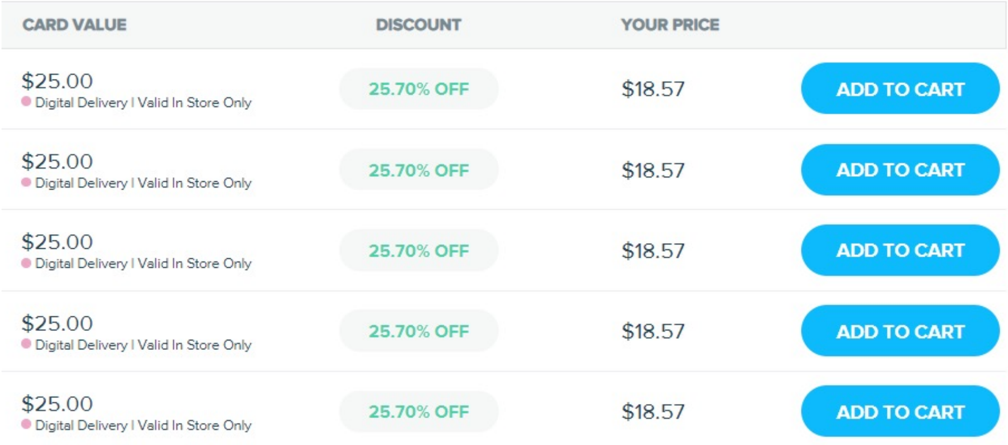
3. Mitigating Social Engineering

In certain circumstances, attackers can bypass otherwise effective safeguards by manipulating or tricking customer service representatives using a technique known as social engineering. In one example the OAG discovered, attackers were able to repeatedly bypass an online retailer's MFA by convincing customer service personnel to send an authentication code via online support chat, instead of by email. Attackers used the authentication code to place orders to a new shipping address using the customer's stored credit card information. In another example, attackers bypassed the re-authentication that would normally be required for delivery to a new address by calling customer service and requesting delivery to a new address after completing a purchase.

Most businesses should develop policies that anticipate social engineering attacks and train relevant personnel on those policies. In the examples described above, policies that prohibited customer service personnel from disclosing authentication codes via online chat or from re-routing orders without re-authentication would likely have mitigated the fraudulent transactions. Businesses can test the effectiveness of these policies and training through simulated social engineering attacks.

4. Preventing Gift Card Theft

Branded stored value cards, also referred to as gift cards, can be an attractive target for attackers. Unlike credit cards, gifts cards are not inextricably linked to a particular customer, so they can often be used by whoever holds them. Moreover, some retailers permit gift cards, or the balances on gift cards, to be transferred directly from one customer account to another. In addition, companies have historically used weaker measures to secure gift cards, permitting their transfer and use without re-authenticating the customer or attempting to determine whether the transaction is fraudulent. As a result, attackers have been able to sell stolen gift cards or gift card balances on the dark web, or even on legitimate gift card resale websites.



CARD VALUE	DISCOUNT	YOUR PRICE	
$25.00 ● Digital Delivery | Valid In Store Only	25.70% OFF	$18.57	ADD TO CART
$25.00 ● Digital Delivery | Valid In Store Only	25.70% OFF	$18.57	ADD TO CART
$25.00 ● Digital Delivery | Valid In Store Only	25.70% OFF	$18.57	ADD TO CART
$25.00 ● Digital Delivery | Valid In Store Only	25.70% OFF	$18.57	ADD TO CART
$25.00 ● Digital Delivery | Valid In Store Only	25.70% OFF	$18.57	ADD TO CART

Stolen gift cards on gift card resale websites can be indistinguishable from legitimate listings

Businesses should ensure they maintain reasonable safeguards to prevent the theft of stored value cards and associated funds. Most importantly, transferring gift cards between customer accounts, and transferring funds between gift cards, should be restricted or require re-authentication. In addition, businesses should obfuscate gift card numbers by, for example, displaying only the last four digits of the gift card number, much like a credit card number.

D. Incident Response

Every business should have a written incident response plan in place that includes processes for responding to credential stuffing attacks. These processes should include, at a minimum, investigation, remediation, and notice.[7]

1. Investigation

When a business has reason to believe that customer accounts have been targeted in an attack, it should conduct a timely investigation. The investigation should be designed 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.

Effective monitoring can greatly reduce the time and resources necessary for an investigation. For example, some bot detection technologies can be configured to allow for the rapid identification of customer accounts that have been impacted in an attack.

Practice Tip

In a recent data breach investigation, the OAG found that engineers at a well-known company failed to investigate a series of credential stuffing attacks after assuming they were merely denial of service (DoS) attacks.

Businesses should ensure that appropriate personnel are trained to recognize the signs of a credential stuffing attack.

2. Remediation

When a business has determined that customer accounts have been, or are reasonably likely to have been, accessed without authorization, it should act quickly to block attackers' continued access to the accounts. In most cases, this requires immediately resetting the passwords of accounts that were likely impacted in the attacks. In some cases, it may also be appropriate to freeze the relevant accounts.

In some situations, it may not be possible for a business to determine with certainty whether certain accounts or certain data were accessed by attackers. In these cases, the business should treat as compromised any account or data that is reasonably likely to have been compromised.

The business should also take steps to defend against similar attacks in the future by closing whatever gaps in existing safeguards attackers exploited to gain access to customer accounts.

[7] This document is not intended to be a comprehensive guide to incident response and covers only those aspects of incident response that are unique to credential stuffing attacks.

3. Notifying Customers

In most cases, businesses should quickly notify each customer whose account has been, or is reasonably likely to have been, accessed without authorization. Notice enables customers to take steps to protect themselves, such as reviewing their online accounts and associated financial accounts for fraud and securing other online accounts that use the same compromised login credentials.

The notice should clearly and accurately convey material information concerning the attack that is reasonably individualized to the customer.[8] This would require, at a minimum, disclosing whether the particular customer's account was accessed without authorization, and, more generally, the timing of the attack, what customer information was accessed, and what actions have been taken to protect the customer.

In some cases, it may be appropriate to contact customers before an investigation has concluded. In these cases, the business should disclose that the investigation is ongoing and, if appropriate, that certain findings are tentative and may change as further information is developed.

Conclusion

The explosive growth of credential stuffing shows no signs of abating, fueled by the ever-growing numbers of stolen credentials that are available to attackers. However, companies can significantly mitigate the risks of credential stuffing to their business and their customers by maintaining a comprehensive data security program with the right mix of cybersecurity measures.

[8] In certain circumstances, existing federal and state law may mandate the method, content, and timing of notice. This guide should be interpreted in a manner that is consistent with those laws.