

SpyCloud

Solution Brief

Prevent Online Fraud with
SpyCloud Consumer Account
Takeover Prevention

OVERVIEW

REDUCING ACCOUNT TAKEOVER AND ONLINE FRAUD WITH SPYCLOUD

KEY FEATURES & BENEFITS

HOW IT WORKS

SUMMARY

SpyCloud protects billions of consumers from account takeover and online fraud.

Hundreds of global enterprises, including 4 of the Fortune 10, trust SpyCloud to reduce fraud without adding friction for legitimate users.



Solution Brief Overview

Retail fraud losses will exceed \$20 billion this year, and the problem is only getting worse. For retailers, every dollar in fraud losses costs three dollars in recovery costs.¹ Online payment fraud losses are projected to surpass \$206 billion between 2021 and 2025.² The reason for a majority of these losses is simple: in today's digital environment, organizations cannot always be sure their customers are who they say they are.

When your consumers reuse passwords, they become pathways for cybercriminals to commit account takeover (ATO), a common form of identity fraud in which criminals use stolen credentials to gain illegitimate access to a user's account. Bad actors take advantage of consumers' bad password hygiene by testing credentials that have been exposed in data breaches against different online login portals to see how many provide a match. New data breaches occur constantly, giving criminals a steady stream of fresh credentials to test against consumer logins; the newer the breach, the more likely consumers haven't yet changed their passwords.

ATO fuels online fraud losses, making it easy for criminals to take over consumers' accounts and access their personal data, funds, and payment information **without being detected**. Even though consumers put themselves at risk with poor cyber hygiene, the financial and reputational consequences primarily fall on enterprises. Unfortunately, keeping up with the torrent of breach data and pace of attacks represents a challenge few have the resources to manage.

To reduce online fraud and protect consumer accounts at scale, enterprises need to prevent criminals from using stolen data to take over their consumers' accounts and commit fraud. SpyCloud Consumer ATO Prevention allows enterprises to stay ahead of attacks by alerting you when your consumer's data appears on the criminal underground. Early detection of compromised consumer accounts enables you to lock criminals out before damage can be done.

How Much is Account Takeover Costing Your Business?

Account takeover creates both direct and indirect costs for businesses, which can vary substantially by industry and individual enterprise.

SpyCloud Consumer ATO Prevention makes a direct, quantifiable difference to your bottom line.

Speak with our Sales Team or your Customer Success representative to calculate what you could save with SpyCloud and develop a business case for decision makers at your enterprise.

TOTAL COSTS

INVOICE # 000000

Bill to
Business Name
Address 1234,
City, State 1111

PRODUCT DESCRIPTION	PRICE
Chargebacks or direct fraud losses	\$\$\$
Dispute fees and fines	\$\$\$
Lost merchandise	\$\$\$
Customer attrition: customer lifetime value vs cost to acquire new customers	\$\$\$
Brand damage	\$\$\$
Lost customer support time	\$\$\$
Lost fraud investigation time	\$\$\$
TOTAL \$\$\$M	

THANK YOU FOR YOUR BUSINESS

SpyCloud Data

Breach Records

SpyCloud recaptures credentials and PII that have been exposed in third-party data breaches. We share the full context of each record, including the breach source and the actual compromised password. Your business is alerted upon discovery and can easily automate remediation efforts.

Malware-Infected User Records

SpyCloud's recovery efforts also include data siphoned from malware-infected devices. We parse out the victim's username, URL, and password and flag them as 'Critical' severity. Incident response efforts should be immediate, since these accounts are at especially high risk of account takeover and online fraud.

Reducing Account Takeover and Online Fraud with SpyCloud

SpyCloud provides what no other account takeover solution offers: the ability to match credentials against the largest, most up-to-date repository of actionable breach data in the industry. That database continues to grow by a billion assets per month, with a focus on maintaining a high volume of plaintext passwords for enterprises to operationalize. SpyCloud uses human intelligence to infiltrate criminal communities and recapture third-party breach data and botnet records in real-time, often months or years before it is publicly available.

SpyCloud Consumer ATO Prevention puts the power of SpyCloud's database to work for fraud prevention, helping you secure consumer accounts before bad actors have a chance to exploit them. From the time an account is established, SpyCloud checks your consumer credentials against billions of exposed passwords and flags any breach exposures that could put your consumer accounts at risk. Because of the high match rates SpyCloud provides, our customers can directly quantify the value of using SpyCloud to secure customer accounts and prevent online fraud.

With SpyCloud, you can:

- ✓ Reduce consumer fraud at scale by locking bad actors out of consumer accounts before they can steal funds, drain loyalty points, or make fraudulent purchases
- ✓ Shorten the exposure window for criminals to access vulnerable accounts with early notification of exposed credentials
- ✓ Protect your brand from backlash and illegitimate claims that result from successful credential stuffing attacks against your users
- ✓ Increase your team's efficiency by automating account takeover prevention so your teams can elevate their focus to more complex projects

Key Features & Benefits

Reduce Consumer Fraud Risk at Scale

Invisibly lock criminals out of vulnerable consumer accounts

Account takeover drives fraud losses. With access to your consumers' stolen credentials, criminals can make fraudulent purchases, drain rewards points, steal private information, and lock legitimate users out of their own accounts. When an attacker logs in using a valid username and password, and particularly when they are able to bypass multi-factor authentication, it can be challenging for enterprises to detect.

2+
Billion
consumers
protected by
SpyCloud data

SpyCloud helps enterprises reduce fraud by checking user credentials for breach exposures at scale, without adding friction or complicating the user experience. Enterprises can protect consumers invisibly by flagging vulnerable accounts before criminals have a chance to exploit them, only taking action when needed. Enterprises have the flexibility to reset compromised passwords or choose an appropriate step-up authentication path for affected users at different points in the customer journey, depending on their organization's needs.

SpyCloud customers see the benefits of fraud reduction immediately. Each set of exposed credentials represents an account that could have been taken over and used for online fraud – or a consumer who might have walked away from your business. The value of preventing consumer fraud isn't limited to material fraud losses. Consumers take months and even years to establish a trusted relationship with a brand, which can easily be destroyed by a negative experience with account takeover. Consumers whose accounts have been stolen typically require assistance from support staff, which can be time-consuming and costly. For some organizations, the reduction in support center call volume alone is enough to justify their use of SpyCloud.

“

Using the SpyCloud data, we discover anywhere from 3,000 to 11,000 direct matches per hour. Every one of those exposed accounts could have led to account takeover.

– Top 10 Travel Booking Site

Stop High-Risk Attacks Tied to Malware

”

*With SpyCloud's
botnet data, we've
protected thousands
of accounts
representing tens of
millions of dollars of
funds.*

- Global Fintech
Company

Many consumers aren't security-savvy. When a suspicious link or file lands in their inbox, some percentage of consumers will open it regardless of potential warning signs, resulting in serious malware infections. For bad actors, it's disturbingly easy to launch a malware campaign that exploits this behavior. There's a robust market on the criminal underground for anything a potential attacker could need to distribute, manage, and monetize a malware campaign that steals user credentials, including sophisticated malware-as-a-service offerings that provide user-friendly dashboards.

Consumers whose systems are infected with malware are at extremely high risk of account takeover, identity theft, and online fraud, with security teams none the wiser. Attackers know they will have a high success rate with a particular user's data and can often go after big-ticket accounts without getting tripped up by security measures like multi-factor authentication. This type of malware collects not only credentials, but also browser fingerprints, session cookies, personal data, and other information that can help them bypass typical security measures.

Unlike other account takeover solutions, SpyCloud helps enterprises identify malware-infected consumers and take swift action to protect them.

Customer Results

\$10M

**Fraud losses
prevented**

- Global Fintech
Company

Intervene Early to Prevent Fraud Faster

After a data breach, attackers typically restrict access to stolen credentials to a small circle of associates for the first 18 to 24 months, giving them plenty of time to monetize the data and quietly exploit your consumers before allowing that data to leak to a wider audience. During that time, they can systematically target high-value accounts before users, enterprises, or even other criminals know that the passwords have been compromised, giving them a higher chance of accessing and exploiting consumer accounts without being detected.

With SpyCloud, you can shorten that exposure window. SpyCloud researchers infiltrate criminal communities to recover breach data early in the breach timeline, giving you as much notice as possible that your customers' passwords have been exposed — often months or even years before a breach becomes public. By taking action before criminals have a chance to use or distribute the stolen credentials, you can head off both targeted attacks by motivated criminals and automated credential stuffing attacks that criminals can launch at scale.



Without the SpyCloud data, we would be in constant risk for attacks we never saw coming.

– Top 10 Travel Booking Site

Increase Your Team's Efficiency with Automation

Collecting breach data takes time that busy security and fraud teams don't have to spare. SpyCloud makes it easy to integrate our data into existing workflows and applications, increasing the scale of your ATO prevention and providing easy access to breach data that can be operationalized effectively.

Customers consistently report that using SpyCloud has helped them increase their team's efficiency and impact due to the quality and actionability of our recovered data. With API-driven access to SpyCloud's robust database, enterprises can protect more consumers using higher quantities of fresh, actionable data than they could get any other way. Because they can rely on SpyCloud, security teams have more time for high-value projects.

Compared to their previous experiences sourcing breach data manually or through a different provider, even enterprises with significant resources and sophisticated ATO prevention plans in place report a substantial performance improvement with SpyCloud. By freeing up internal resources who previously spent time hunting for breach data, they're now able to apply their time and expertise to other priorities.



I would need a bigger team without SpyCloud.

– Global Managed Services Provider

“

We look at SpyCloud
as a reputation
mitigation as well.
You can do everything
right and still end up
in headlines for the
wrong reasons. At a
certain volume, ATO
is indistinguishable
from your platform's
security being
compromised.

- Global Fintech
Company

Customer Results
20M
Bad passwords
reset

- Global Job Hunting
Company

Protect Your Brand

You can do everything right and still end up in the headlines for the wrong reasons. Malicious actors love to scam each other by compromising accounts via credential stuffing and passing them off as a fresh breach. When that story hits the news, it's difficult for journalists or consumers to distinguish between accounts that were accessed because of weak passwords versus a breach of your corporate network.

SpyCloud helps you prevent negative customer experiences by proving that your brand takes account security seriously. By proactively securing customers' accounts, you can protect your company from false data breach accusations and the negative media attention that results from account takeovers.

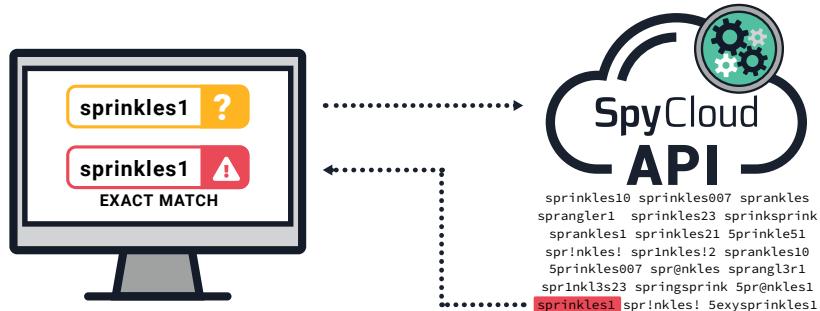
How It Works

SpyCloud Consumer Account Takeover Prevention operationalizes SpyCloud's extensive database of recovered stolen breach assets using two high-volume, performant APIs to identify consumer accounts that are at elevated risk of account takeover and online fraud. Depending on your organization's requirements, you can check consumer logins using identifiers (such as email address, username, phone number, or IP address), passwords (partial hashes), or a combination of both.

- ✓ **Password Exposure API** – Check hashes of your consumers' passwords against all passwords in the SpyCloud database, regardless of username
- ✓ **User Exposure API** – Check the SpyCloud database for breach exposure tied to your consumers' email addresses, usernames, IP addresses, or phone numbers

The two APIs are complementary; they can be used in separate scenarios and offer different protections. Using both APIs together provides the strongest protection against account takeover. Alternative solutions are available for organizations that must satisfy a high volume of API calls or specialized privacy requirements.

Both APIs include easy-to-understand, resource-oriented URLs, and use HTTP response codes to indicate API transaction status. All API responses return JSON, including those with errors.



Customer Results

20%
**Performance
increase**

- Fortune 100
Technology Company

Three Popular Implementations

SpyCloud Consumer ATO Prevention offers flexibility for enterprises to decide how and when to check credentials to identify consumer accounts that are at elevated risk of account takeover and online fraud. Enterprises can choose to block bad passwords from being created, check credentials at the time of login, screen their entire database at regular intervals, or some combination of the three.

Prevent Bad Passwords at the Time of Creation

Head off bad passwords by checking user credentials during account creation, password change and password reset.

Test User Logins in Real Time

Check credentials in real time as users log into your application, in parallel with a step-up authentication procedure for high-risk actions.

Proactively Check Your Entire Database

Check your entire database of credentials on a frequent basis to detect new exposures, whether or not your users have been active.

When SpyCloud identifies that a consumer account is vulnerable, enterprises can choose to intervene in a wide variety of ways depending on their business needs, whether that means locking the account, triggering step-up authentication measures, or even waiting until after a transaction is complete to force a password reset.



“

The fact that SpyCloud is customizable to our needs now but also scalable to where we may go in the future is one of the reasons we chose their solution.

– Top 10 Travel Booking Site

Customer Results

**18+
Months
Early**

***SpyCloud
typically
acquires
breaches
18 months
before they
are publicly
available on
the dark web***

Security and Compliance

SpyCloud uses IP whitelisting to secure access to the API, and all data is encrypted while in transit and at rest. We allow flexibility in the data points returned from our API, allowing you to obscure fields that shouldn't be accessible to your application. In addition, we can further secure the outputs by hashing and salting the values returned to you.

Summary

What would it mean to your enterprise to substantially reduce account takeover fraud that's affecting your customers and your bottom line? For many of our customers, the answer is measured in dollars tied to direct fraud losses. For others, reducing support call center volume provides substantial savings. In either case, our customers are able to quantify significant improvements.

ATO is a business problem that can't be stopped without first addressing a root cause – password reuse. While consumers' bad password habits are typically to blame, organizations are often mistakenly perceived as the irresponsible party. The most straightforward way to prevent ATO is to be aware of consumers with compromised credentials, allowing your organization to proactively decide how and when to act.

Criminals acquire credentials from third-party breaches and malware infections daily, opening the doors to account takeover and hard-to-detect fraud. Businesses in every industry and of every size are at risk, so preventing ATO is imperative.

We encourage you to work with our sales team to understand how SpyCloud Consumer Account Takeover Prevention could support your own fraud prevention objectives – and let us prove the impact SpyCloud can have for you with a data match rate test against your consumer database.

See how SpyCloud can help prevent fraud losses and brand damage caused by ATO.

[Request a Demo](#)