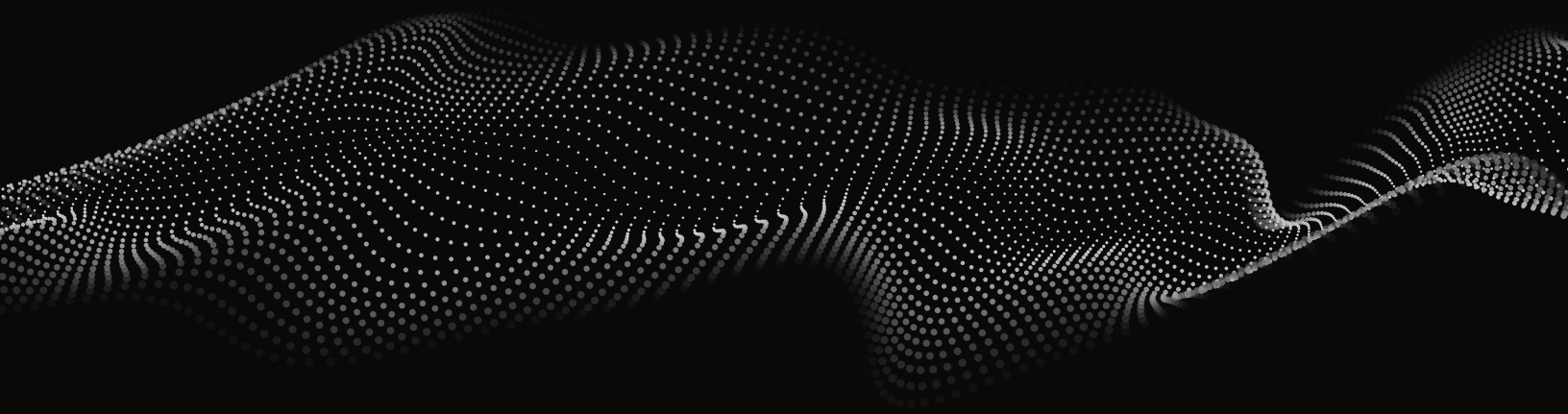
Reducing Identity Fraud While Improving the Digital Customer Experience in Financial Services

Whitepaper

SpyCloud

SpyCloud

Table of Contents



Introduction

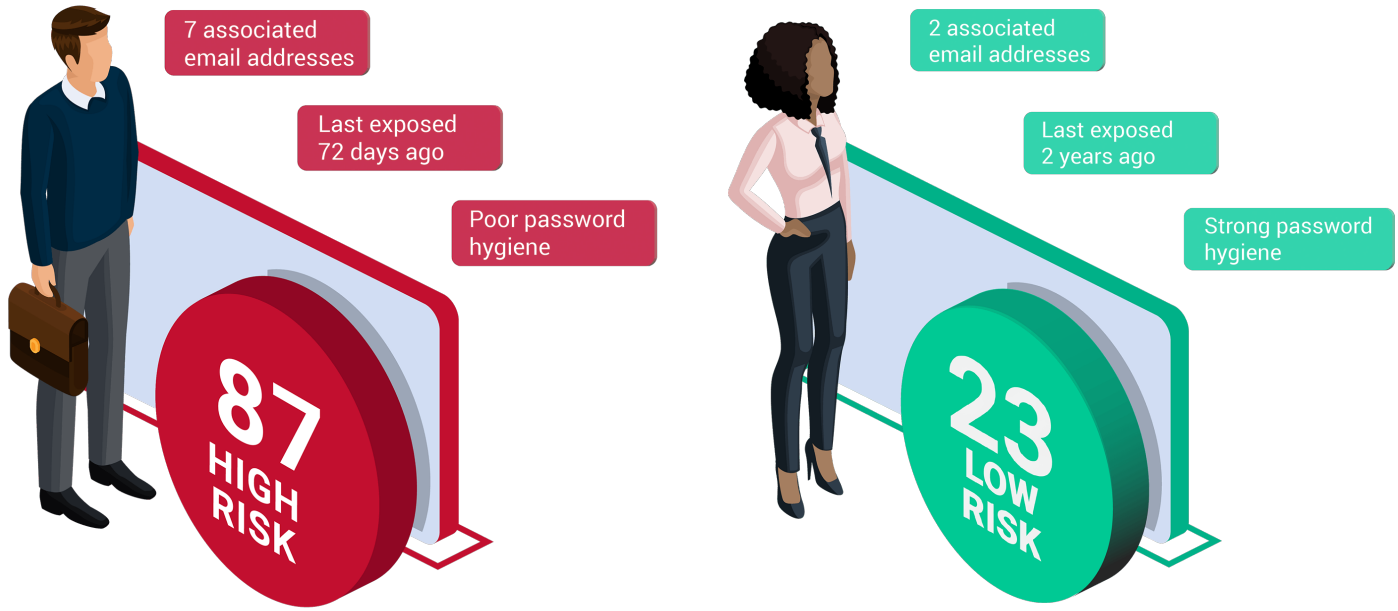
Confirming the identity of account openings and account holders is an expensive responsibility looming over the financial sector. Without proper oversight and controls, it results in massive losses, government fines, and the threat of reputational damage.

The pandemic isolated millions of people in their homes with businesses and financial services desperate to serve them. This condition thrust consumers into a digital revolution with a staggering adoption rate of online payments and banking. A wave of fraud soon followed the explosion of online digital activity. The perpetrators uncovered the weakness of traditional fraud models, leaving financial institutions (FIs) to deal with 85-95% fraudulent applicant attempts.

Consequently, FIs are investing more heavily in fraud detection measures – but they struggle to keep up with the evolution and ramifications of identity theft and related threats, including their increased prevalence and sophisticated methods of attack.

One of the biggest challenges for the sector is the need to balance efficiency and positive customer experiences from the application process through to the transaction while seamlessly deflecting fraud. Customers expect fast, frictionless, real-time online interactions, and although FI customers are less fickle than e-commerce ones, they won't hesitate to seek other services if they are faced with ongoing barriers.

But how do you establish trust when not all customers bring equal risk? Putting low-risk customers through the same rigorous verification steps as high-risk ones is not only unnecessary, it's expensive and leads to loss of business. Fortunately, new tools enable FIs to mitigate identity theft risks while streamlining the user experience.



The State of Identity Fraud

Account takeover and new account opening and application fraud have long plagued the financial services sector. To fight back, FIs have been deploying more controls. Yet cybercriminals continue to find new and novel ways of perpetrating digital fraud.

In the past year, 84% of surveyed FIs have experienced account takeovers. The top consequences of these fraudulent activities for FIs included:

- Fraudulent transactions (experienced by 45% of FIs)
- New accounts creation (31%)
- Transfer of funds or fungible value (24%)

Losses resulting from stolen identities across all industries grew 43% in the US, from $502.5 billion in 2019 to $712.4 billion in 2020. While the COVID-19 schemes that fueled much of that growth are expected to abate, identity thieves will continue to exploit new global trends.

For example, 35% of consumers have increased their use of online banking as a result of limited mobility during the pandemic. The changes in consumer behaviors and stronger reliance on online transactions create a fertile ground for identity fraud. In the first quarter of 2021, online banking transactions accounted for 96% of FIs' activity – and were also the most targeted attack surface, accounting for 93% of all fraud attempts.

Average FI customers – even those who are more technically savvy – are dependent on organizations to protect their account information to prevent fraud. Consumers often:

- Use poor cybersecurity hygiene such as weak or reused passwords
- Conduct online transactions on devices that don't have adequate security
- Lack awareness about the latest social engineering and phishing techniques

Bad actors, in turn, recognize that it's much easier to target this growing number of digital services consumers rather than trying to circumvent FIs' security controls. Although the financial sector itself sees its fair share of cyberattacks, the customers – not the FI's security vulnerabilities – have become the weakest link.

The Most Common Forms of Application Fraud

- Opening a checking account
- Obtaining a credit card
- Procuring a mobile phone

(Source: Aite, "US Identity Theft: The Stark Reality," 2021)

Customers, however, expect their FI to protect them from the nefarious activity, with 53% saying it's the FI's job (vs. 47% putting the onus on government and 40% on themselves). And they don't hesitate to walk away if they feel the institution is not adequately protecting their data and privacy.

There is no end in sight to digital fraud. The abundance of cheap PII and stolen credentials on the dark web, coupled with the automation that fraudsters employ, makes online fraud a lucrative gig. And the skyrocketing number of data breaches create a snowball effect that will keep exacerbating account takeovers and new account fraud – continuing to challenge FIs' ability to stay a step ahead.

Hard-to-Detect Fraud: You Can't Prevent What You Can't See

Fraud detection solutions are advancing in their sophistication. One aspect they miss, however, is how malware amplifies risk exposure. When a customer's computer or device is infected, all of the data and activity on that system is at the fraudsters' fingertips, enabling them to:

- Steal PII, credentials, and other information
- Log into various accounts, including email and banking, and make changes
- Bypass logins altogether in some cases, and even multi-factor authentication (MFA)
- Collect information they can use for social engineering or phishing
- See any changes, like replaced passwords, and sell the updated data on the dark web
- Emulate a legitimate customer's browser or device fingerprint

Infected systems create an extreme risk for online fraud and identity theft. Malware provides the proverbial keys to unlocking the kingdom – and as long as the system remains compromised, measures like resetting passwords and even applying MFA are not fully effective. Mitigating this risk for FIs requires additional monitoring and scrutiny, and it starts with gaining visibility into fraud tied to malware.

Two Types of Identity Fraud FIs Need to Mitigate

1) Account Enrollment or Account Opening Fraud:

Fraudsters open accounts using stolen or fabricated identities by:

- Impersonating a legitimate consumer ("true name fraud") using what's known in the industry as fullz, or full packages of a person's data for sale on the criminal underground
- Mixing a patchwork of fake information and authentic data from different profiles to create a synthetic identity

Victims or credit issuers often don't become aware of this type of scam until the account is sent to collections.

Research shows that synthetic identities resulting from application fraud is the type of attack FIs are concerned about the most – with 52% of surveyed FIs expressing their worry about adequately detecting attacks and preventing losses stemming from these threats.

2) Account Takeover (ATO):

Cybercriminals can take over existing accounts in a variety of ways, including by:

- Buying validated credential pairs (usernames and passwords) from underground marketplaces
- Launching automated, high-volume credential stuffing attacks using commodity logins found on the dark web from previous breaches
- Infecting consumer devices with malware and harvesting browser fingerprints, PII, credential combinations, and other data

Once inside, the fraudster will change the password and the user's PII, locking the account to drain funds or activate new services.

ATO attacks take advantage of massive amounts of breached credentials and high rates of reused passwords among consumers.

In 2021 alone, SpyCloud recaptured 1.7 billion credentials from the criminal underground, and found a 70% password reuse rate among users with more than one exposed password.

The Role of Underground Data

It's no secret that data breaches and malware campaigns have created a massive treasure trove of stolen data that cybercriminals operationalize in numerous, innovative ways. What's less understood by many FIs is that underground data is at the core of identity fraud attacks. Breached and malware-siphoned data that has been recaptured and analyzed can tell a story of the different levels of customer risk.

The Identity Theft Resource Center identified 1,108 publicly disclosed data breaches in 2020. By the third quarter of 2021, the number of breaches exceeded 2020 by 17%.

Even compromised credentials – criminals' most sought-after type of data – come into play differently depending on how "fresh" they are. Before leaking or selling logins to others in the underground (to be exploited for credential stuffing attacks), cyberthieves first use them for targeted attacks on high-value accounts.

Immediately after obtaining the credentials, the bad actors share these newly harvested credentials with a very small and trusted network that can launch attacks. Humans, rather than bots, initiate these attacks to avoid detection. The compromised credentials don't make it to the underground marketplaces for months and often several years, at which point they become commodity data used for credential stuffing attacks – sold at bargain prices or even given away.

Stolen credentials used during the early, targeted attack phase pose a very high risk to FIs. Yet solutions designed to monitor the dark web for compromised data won't find these logins since they haven't been shared widely yet. In the meantime, armed with these credential pairs and tactics such as social engineering to subvert logins, MFA and other mechanisms, cybercriminals can gain access to high-value accounts and drain them before the FI or the consumer realizes something is wrong.

Common Attack Scenarios

Cybercriminals benefit from stolen underground data at three main stages of the customer journey:

- **New account opening:** The fraudster establishes a new account with a fullz record from the criminal underground or by piecing together stolen data to form a synthetic identity. Without any previous or negative history, the account application will not trigger red flags via the typical fraud detection mechanisms. The fraudster may leave the account dormant at first but will then gradually build trust with the FI before eventually making high-end purchases with no intention to pay off the debt. This is called "busting out fraud."
- **Account login:** The fraudster obtains stolen credential pairs or uses malware to harvest logins directly from the consumer's device. As described earlier, these ATO events can result from either targeted or credential stuffing attacks. Once in, the bad actor can initiate actions such as transferring funds or changing the mailing address, then ordering debit cards or checks.
- **Account modification:** Using similar ATO tactics to gain access to the account, the fraudster can completely lock out the legitimate customer by changing the notification settings and all the contact information. The account holder doesn't see any red flags since all the notifications have been diverted.

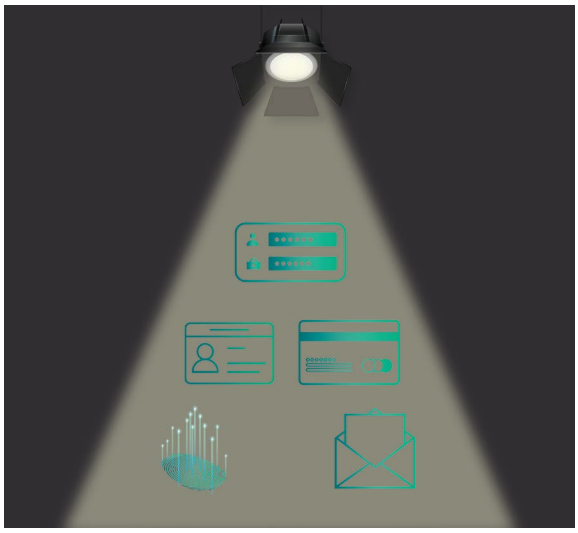
Only about 10% of credential-based attacks are classified as targeted, yet they cause 80% of losses.

(Source: SpyCloud Customer Advisory Board)

A Common Misconception

FIs may wonder – isn't underground data only valuable to cybercriminals? FIs can use refined and recaptured data to gain insight into a customer's level of risk and fight back. Data that establishes the timing and type of the exposure are just a couple of factors to consider when predicting a customer's level of risk so you can make smarter transaction decisions.

Impact of Key Risk Indicators



Across the last 5 years, SpyCloud has recaptured more than 145 billion assets from data breaches, malware-infected devices, and other underground sources. It's not a stretch to say that data breaches have impacted most consumers by now – and everyone is at risk of fraud to some degree. But not all risk posed by their exposure is equal.

Some of the factors that impact risk exposure include:

- The timeline or age of the data exposure and the frequency of exposures
- The type of data exposed (e.g., leaked SSNs that facilitate synthetic identity creation or phone numbers that increase ATO risk, since many consumers use them to verify and authenticate their identities)
- Consumer devices infected with malware
- Rates of password reuse
- Suspicious correlations (e.g., multiple dates of birth linked to an email address may indicate a synthetic identity)

Understanding customers' underground risk profile and the context of the exposures they have experienced helps FIs proactively detect and prevent fraud faster and with greater accuracy. Intelligence such as breach data, stolen PII, logs from credential-stealing malware, and security hygiene – among other data points – can help differentiate trusted customers from risky ones.

By using this intelligence and better knowing your customers, you can predict user risk. This enables you to manage each customer's transaction experience with the appropriate journey, avoiding process interruptions, more closely monitoring certain interactions when necessary, and making fraud decisions upfront to create a more seamless overall interaction.

Why Risk Exposure Matters to FIs

The climbing numbers of both online users and fraud losses compels FIs to invest into more fraud and authentication solutions. These solutions add not only cost but also unnecessary friction for legitimate customers' experiences. Establishing trust levels across the board leads to less false positives, delays, manual reviews, and customer disruption – which, in turn, contribute to customer dissatisfaction, churn, and further costs.

The majority of consumers have the expectation that FIs have the highest level of security to protect accounts while maximizing their user experience. And while 55% believe security is the most important aspect of their online experience, many also say they would abandon a transaction that takes more than 30 seconds. This emphasizes the need for FIs to implement seamless and fast fraud analysis tools, balancing prevention controls and fraud mitigation with the customer experience.

> **59% of surveyed US consumers and 60% of UK consumers want businesses to implement strong, invisible security measures.**

How SpyCloud Identity Risk Engine Detects Risky Consumers

As fraud practitioners know, there will never be one silver bullet for fraud prevention. In an attempt to differentiate between legitimate consumers and criminals, businesses layer anti-fraud solutions into their control frameworks, likely unaware that the missing link to detect digital identity fraud is visibility into the underground exposed user data that enables fraudsters to bypass traditional fraud models.

SpyCloud Identity Risk Engine provides actionable, predictive fraud risk assessments based on data recaptured from the criminal underground using human intelligence. SpyCloud's engine draws on billions of data points to evaluate each FI customer's risk exposure and identify those with the highest risk of identity fraud.

FIs can query the SpyCloud API at vulnerable points in the customer journey, such as new account opening, login, and account modification, using the customer's email address or phone number. The SpyCloud engine correlates the underground data linked to the customer, assesses the key risk indicators, and returns a risk score along with supporting information that explains the score and can be adjusted according to the FI's risk tolerance.

Let's look at two scenarios, one high risk and one low risk:

Scenario #1:

1. A fraudster applies for a new account with a synthetic identity that's a composite of several legitimate consumers. An identity verification solution validates the identity because it finds an exact match for some data, such as the name, IP address, geolocation, and device ID.
2. SpyCloud Identity Risk Engine is queried and returns a risk score of 87, having correlated the data for that user among its vast database. SpyCloud identifies that the same email address is associated with several other names and devices, and the date of birth and Social Security number are associated with another person's mailing address, email, and password. SpyCloud also identifies that some of the applicant's data was recently exposed on the underground.
3. The SpyCloud score of 87 indicates a high level of risk and the reason codes and metadata support the risk score.
4. Based on its internal rules, the FI flags the application for manual review or blocks the transaction.

Scenario #2:

1. Someone is trying to log into an account and the FI wants to ensure this is a legitimate customer. The FI queries SpyCloud Identity Risk Engine at login.
2. SpyCloud delivers a risk score of 23 along with up to 20 reason codes and metadata as supporting information showing that the customer's email and password were exposed in a third-party breach nearly a year ago and the user has only a 10% password reuse rate. The query doesn't surface any other data indicating high-risk exposure, such as malware on the customer's device.
3. The SpyCloud score of 23 indicates a low risk and the reason codes and metadata support the risk score.
4. Based on its internal threshold for risk, the FI automatically allows the customer to proceed without additional verification, enabling a seamless and fast login.

SpyCloud Identity Risk Engine allows you to make confident, real-time decisions – eliminating unnecessary friction, preventing churn, and reducing fraud losses. The key benefits of the solution include:

- ✓ Identifying high-risk customers early in the lifecycle at the points most vulnerable to fraud
- ✓ Stopping the hard-to-detect fraud tied to malware infections
- ✓ Promoting customer longevity by proactively taking action on high-risk accounts
- ✓ Streamlining the digital experience by allowing trusted users to bypass unnecessary verification steps
- ✓ Increasing efficiency and expediting fraud decisions by reducing manual review time

SpyCloud

Balancing Fraud Prevention with Customer Satisfaction

As digital adoption advances and identity theft evolves, FIs need to seek out new ways of achieving the right balance between fraud prevention and customer experience. If your fraud technology fights fraud at the expense of customer satisfaction, your risk controls and your business goals will always conflict with each other.

Customer loyalty and trust are among the top factors that drive your business forward. With consumers expecting more from their service providers and online interactions, creating a seamless customer journey is a priority for FIs. An effective fraud solution that incorporates identity intelligence ensures that you can meet this priority without negatively impacting your risk.

SpyCloud turns the table on fraudsters by making criminal underground data work for FIs and enabling them to make faster, more confident fraud decisions. By using the SpyCloud Identity Risk Engine, you can make these decisions at scale and customize your customers' journey to minimize friction while mitigating your fraud risks.

About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include 4 of the 10 largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 150 cybersecurity experts who aim to make the internet a safer place.

Identity Risk Engine

Detect your consumers' risk of account takeover, synthetic identities, and fraud tied to malware.

Learn More

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized transactions.

Learn More

Employee ATO Prevention

Protect your agency from breaches and ransomware attacks.

Learn More

VIP Guardian

Protect your highest-risk users from targeted account takeover.

Learn More

Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More

Third Party Insight

Monitor suppliers' exposures and share data to aid in remediation.

Learn More

SpyCloud