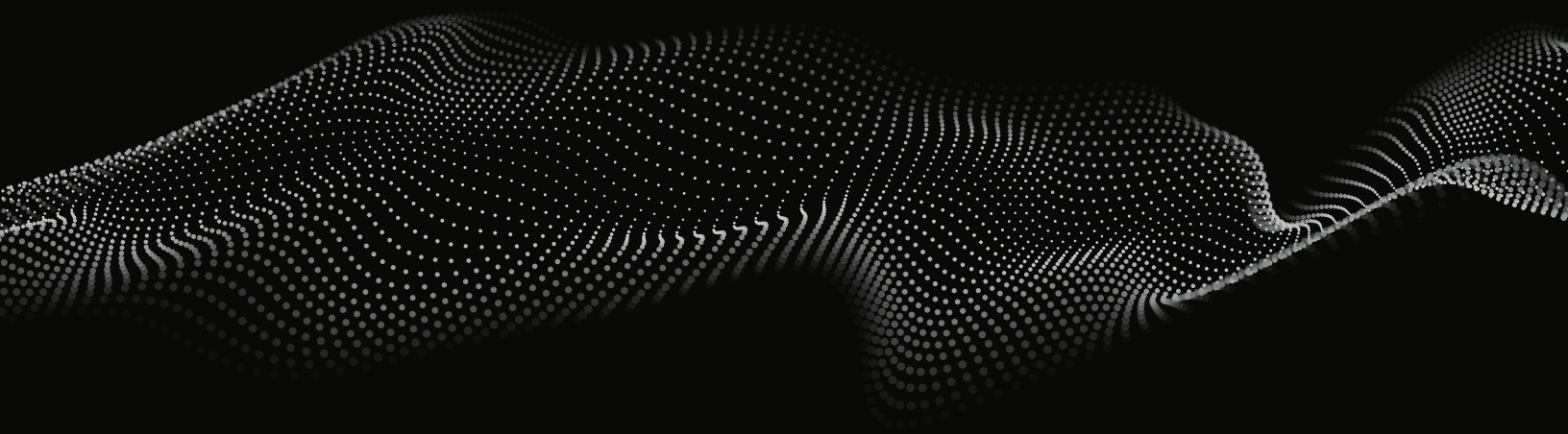
WHITEPAPER

Reducing Identity Fraud in Ecommerce

Balancing Fraud Losses & Customer Experience

SpyCloud

Table of Contents



Introduction

Online identity fraud has become a larger share of fraud losses for retail and ecommerce merchants, creating more pressure on confirming the identity of new and existing customers. The lack of the right controls can lead to lost sales, high fraud mitigation costs, and negative brand reputation – with every $1 of fraud costing U.S. merchants $3.75 (compared to $3.36 in 2020).

The top two challenges ecommerce companies face today are online identity verification and balancing fraud prevention with customer friction. The new digital era ushered in by the pandemic exacerbated these challenges, as both customers and fraud perpetrators flocked online.

The pandemic has changed more than customer habits — it has forced many to transact online. More than half of consumers (55%) say the crisis has raised their customer service expectations, and 79% believe their experience with a company is just as important as the product or service they're buying. This means the ecommerce sector needs to find new ways of reducing customer friction, from the opening of a new account through checkout, while detecting fraud seamlessly and cost-efficiently.

Yet fraud team resources have not kept pace with the growth in online shopping and fraud attacks. So how can these teams maintain low transaction review rates and low false declines while making fast, accurate fraud decisions and minimizing the risk of chargebacks and other fraud?

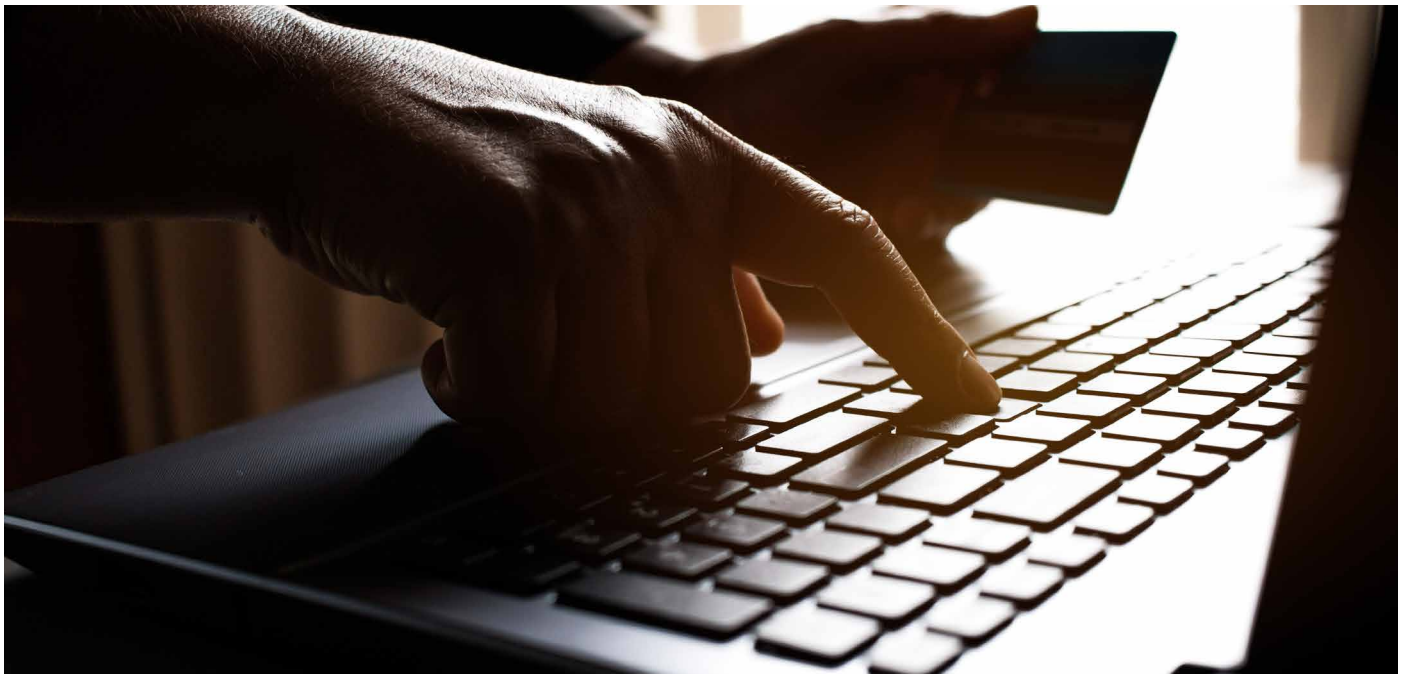
Taking all customers through the same rigorous verification steps is not only expensive but also results in lost sales and customer churn. Fortunately, new tools enable ecommerce companies to differentiate between low- and high-risk customers, so they can balance fraud mitigation and the user experience.

Top Online Fraud Challenges of North American Retailers*

- Customer identity verification
- Balancing fraud prevention with customer friction
- Email or device verification
- Phone verification
- Address verification

**North American Retailers*

(Source: LexisNexis, "The True Cost of Fraud," 2021)



The Evolution of Ecommerce Fraud

Online shopping became a lifeline for consumers isolated at home during the early stage of the pandemic. In just a few months, ecommerce saw 10 years' worth of growth. But even when in-person shopping fully resumed in the first half of 2021, ecommerce traffic spiked 51% compared to the same period the previous year.

As consumers turned to online merchants, so did fraud perpetrators. The ecommerce sector experienced an 140% increase in the volume of fraud attacks in 2021 compared to pre-COVID, and three out of four surveyed merchants reported an increase in fraud attempts and related attacks.

These trends will not improve anytime soon. Ecommerce will continue to boom, considering that 91% of consumers who increased their online shopping said they'll likely continue doing so in the future. As long as consumers embrace ecommerce, so will fraudsters.

The escalation of data breaches and malware infections has made cheap PII and stolen credentials even more abundant on the criminal underground, while off-the-shelf automation products make fraud a low-skill yet lucrative occupation. Staying ahead of the fraudsters will require tactics that evolve in step with the fraud landscape.

Three Types of Identity Fraud Ecommerce Companies Need to Mitigate

Guest Checkout Fraud:

Criminals evade detection and commit fraud via guest checkout by:

- Bypassing identity verification checks due to the lack of account history, historical data, or purchasing behaviors that would otherwise flag suspicious activity.
- Purchasing identity kits and using a legitimate person's name, payment method, and billing address to clear basic public database checks, but shipping to a mule address where they can receive the products.
- Using stolen payment information and choosing rushed shipping, in the hope that they will receive the product before the victim notices and can dispute the charge.

Many organizations struggle when deciding to implement guest checkout as an option for their customers. Ease and speed of transaction are important to consumers, with 24% reporting they will abandon online transitions because of mandatory account creation. While user experience and preventing revenue loss are critical, businesses must prepare as criminal tactics evolve and CNP fraud continues to rise and losses are estimated at $130 billion in cumulative revenue by 2023.

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 steal loyalty points or divert merchandise orders to a new address. Nearly a quarter of identity-related fraud in North America was related to ATO in 2021. Additionally, every 1 in 140 login attempts during the 2021 holiday season was an ATO attempt.

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

New Account (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
- Obtaining raw payment card data stolen using that data (known in the industry as dumps) for card-not-present (CNP) fraud
- Mixing a patchwork of fake information and authentic data from different profiles to create what's called a synthetic identity

According to FIVerty, as many as 50% of new US accounts created in 2021 were fraudulent.

The total identity fraud impact, by combining traditional identity fraud and identity fraud scam statistics, resulted in $52 billion of loss affecting 42 million U.S. consumer victims.

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 are at the fraudsters' fingertips, enabling them to:

- Steal PII, credentials, and other information
- Log into various accounts, including email and online shopping, 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 merchants requires additional monitoring and scrutiny, and it starts with gaining visibility into fraud tied to malware.

How Fraudsters are "Innovating"

Buy online/pick up in store (BOPIS) has become a popular option for consumers, with recent studies suggesting that by 2024, 40% of all sales in the US will be generated via BOPIS and the market will exceed $140 billion.

Fraudsters are taking notice of this growing trend. BOPIS fraud is more difficult to detect because there's no delivery address to verify the buyer's identity. Stores typically try to fill these orders as fast as possible, which also shortens the review time.

After a dramatic spike in 2020, BOPIS sales continued to rise at an estimated 15% in 2021, indicating that many consumers continue to prefer this hybrid experience.

The Role of Underground Data in Fraud Schemes

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 merchants 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.

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.

Immediately after obtaining the credentials, the bad actors share these newly harvested credentials with a very small and trusted network that can launch attacks on high-value targets. 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 ecommerce companies. 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 customer accounts and drain them of loyalty points or place high-ticket orders before the consumer realizes something is wrong.

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%.

Common Attack Scenarios

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

- **New account opening:** In one scenario, the fraudster establishes a new account with a newly created email, password and burner phone, as well as stolen payment card data complete with the CVV. The fraudster will either place orders immediately or wait for the account to age and become established to build trust. In another scenario, the fraudster pieces together stolen data to form a synthetic identity and apply for a store credit card. Without any previous or negative history for that identity, the account application will not trigger red flags via the typical fraud detection mechanisms and the store will issue a credit card. The fraudster will slowly build credit history by making a series of small orders, working toward a higher credit limit before eventually making high-end purchases with no intention to pay off the debt. This is called "busting out fraud."
- **Account login:** The fraudster takes over a shopping account with credential pairs obtained on the criminal underground or harvested from the consumer's device with malware. As described earlier, these ATO events can result from either targeted or credential stuffing attacks. Once in, the cybercriminal can change the mailing address and order merchandise. Another common ATO scheme is to steal loyalty points or gift card balances, which the fraudsters can monetize on the underground.
- **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.

One of the biggest misconceptions about underground data is that it's only valuable to cybercriminals. However, ecommerce companies can use the refined and recaptured data to gain insight into a customers' level of risk and fight back. Key risk indicators and data points that establish the timing and type of the exposure are just a couple of factors to consider when predicting a customer's risk so you can make smarter transaction decisions.

43% of surveyed U.S. merchants said that more than 10% of their fraud chargebacks were the result of ATO.

Risk Exposure and Why It Matters in Ecommerce

Since 2016, SpyCloud has recaptured more than 250 billion data points from over 10,000 data breaches. 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 merchants proactively detect and prevent fraud faster and with greater accuracy. Intelligence such as breached data, stolen PII, logs from credential-stealing malware, and customers' security hygiene – among other data points – helps differentiate trusted customers from risky ones.

By using this intelligence during the weakest point of the transaction cycle, you can predict user risk. This enables you to manage each customer's transaction experience with the appropriate journey, avoiding process interruptions, minimizing unnecessary manual reviews, and making fraud decisions upfront to create a more seamless overall interaction.

Why Risk Exposure Matters

The cost of fraud continues on an upward trajectory. Close to 40% of surveyed ecommerce merchants lost at least 6% of revenue on payment fraud in 2020. So it's not surprising that nine out of 10 merchants now consider managing ecommerce fraud an important part of their business strategy, and spending on fraud management has increased five-fold since 2019.

Yet ecommerce companies are still struggling to get fraud under control. Identifying and responding to emerging fraud attacks is the second biggest challenge in ecommerce. Additionally, false positives further erode revenues. While losses due to ecommerce fraud reached an estimated $6.4 billion in 2021, losses due to false declines were estimated to top those by 70x, totaling a staggering $443 billion.

Part of the challenge is that common fraud and authentication solutions add not only cost but also unnecessary friction for legitimate customers' experiences. As noted earlier, consumers now have much higher expectations of their interaction with brands. By establishing trust levels for individual customers, you can reduce false positives, manual reviews, and customer disruption – which, in turn, improves customer satisfaction, reduces churn, and cuts costs.

You can establish trust by using the underground data to your advantage. When you distinguish between customers who pose different degrees of risk, you make fast and accurate decisions with a higher degree of confidence in real time.

How SpyCloud Identity Risk Engine Detects Risky Customers

As anti-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 exposed user data that enables fraudsters to bypass traditional fraud models.

SpyCloud Identity Risk Engine provides what no other anti-fraud solutions can: actionable, predictive fraud risk assessments based on data recovered from the criminal underground using human intelligence. SpyCloud's engine draws from the world's largest database of underground data, comprised of billions of data points, to evaluate each ecommerce customer's risk exposure and identify those with the highest risk of identity fraud.

Merchants 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 the reason codes and metadata that explain the score and can be adjusted based on your company's risk threshold.

Globally, ecommerce companies allocate 36% of their fraud budgets to manual reviews (less than in previous years); however, 53% plan to reduce them and 12% plan to eliminate them altogether.

Let's look at two scenarios, one low risk and one high 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 merchant flags the application for manual review or blocks the transaction.

Scenario #2:

1. Someone is trying to log into an account and the merchant wants to ensure this is a legitimate customer. The company queries the SpyCloud Identity Risk Engine at login.

2. SpyCloud delivers a risk score of 20 and supporting information showing that the customer's email and password were exposed in a third-party breach nearly a year ago and the user only has 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 20 indicates a low risk and the reason codes and metadata support the risk score.

4. Based on its internal threshold for risk, the merchant 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 with actionable intelligence and predictive fraud risk assessments. The key benefits of the solution include:

- ✓ Improving the accuracy of fraud decisions and reducing the likelihood of false declines
- ✓ Reducing chargebacks by flagging users whose risk exposure make them most vulnerable to fraud like ATO
- ✓ Stopping new account fraud without blocking legitimate signups
- ✓ Increasing efficiency and expediting fraud decisions by reducing manual review time

SpyCloud turns the table on fraudsters by making recaptured data work for ecommerce companies – distilling actionable insights from more than 145 billion data assets recovered from the criminal underground. By using the SpyCloud Identity Risk Engine, you can make fast, confident decisions at scale and customize your customers' journey to minimize friction while mitigating your fraud risks.

SpyCloud

Balancing Fraud Prevention with Customer Satisfaction

Despite the growing fraud losses, more ecommerce companies are now choosing to prioritize improving their customer experience over fraud reduction. As ecommerce continues to thrive, customer experience will play a more significant role in driving revenues. But achieving this goal at the expense of fraud prevention is not a sustainable model.

An effective fraud solution that incorporates identity intelligence will help you balance risk controls with customer satisfaction. The right technology can eliminate the conflict between risk mitigation and business goals – ensuring you can meet both priorities equally.

About SpyCloud

SpyCloud transforms recaptured data to protect businesses and consumers 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 customers 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 half 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.

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More

SpyCloud