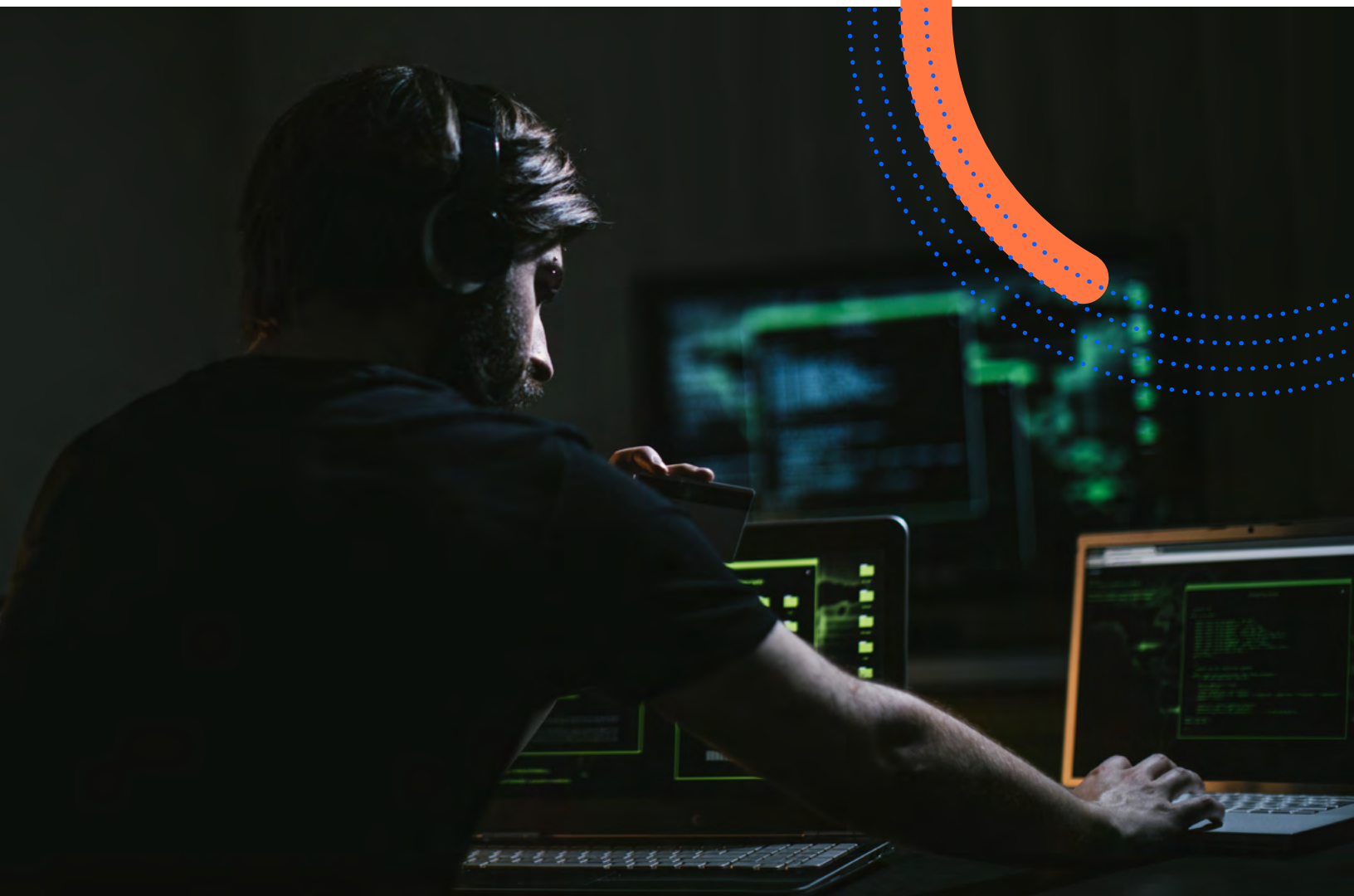
Verisk

Identity Fraud:

How digital deception is reshaping insurance risk

By **John Trovinger**, CPCU, CLU; AVP Client Success and **Shay Gause**, CFE, MBA; Sr. Director Consulting



Digital deception is no joke

Fans of comedian Jim Carrey might recall his *Ace Ventura: Pet Detective* films and his myriad roles and "identities," culminating in his film *Me, Myself, and Irene*. But there's nothing comedic in the serious and complex role of identity in today's digital world. As daily life continues to be increasingly intertwined with online platforms, accurate and secure identity care and resolution has never been more critical within the property and casualty industry.

From broad data breaches to the dark web, and from account takeovers to falsified claims, the pace of digital innovation is proving to be a massive, ever-evolving threat. This white paper explores the growing challenge of stolen and fabricated identities, their impact on property and casualty carriers, and strategies to mitigate that impact.

Today's fraudster

Today's digital fraudsters may be the equivalent of the bank robbers of old, but able to steal more with less risk of prosecution because it's easier to remain anonymous and operate from anywhere in the world. Online applications, with remotely filed claims and user-submitted digital evidence such as photos, receipts, and claim documents, have revolutionized insurance workflows. While these innovations aim to reduce cycle times, maximize customer satisfaction, and boost employee efficiency, they can be a fraudster's dream with the ease of obtaining or accessing coverage, filing claims, and receiving payment. Many communications occur without ever meeting or talking directly with an insurance representative.

One example of the growing threat is account takeover (ATO) fraud. First emerging in the financial and life insurance/retirement sectors, ATO often involves a stolen identity and increasingly affects property and casualty insurers too. Add to this the emergence of synthetic identities, and the risk grows greater still.

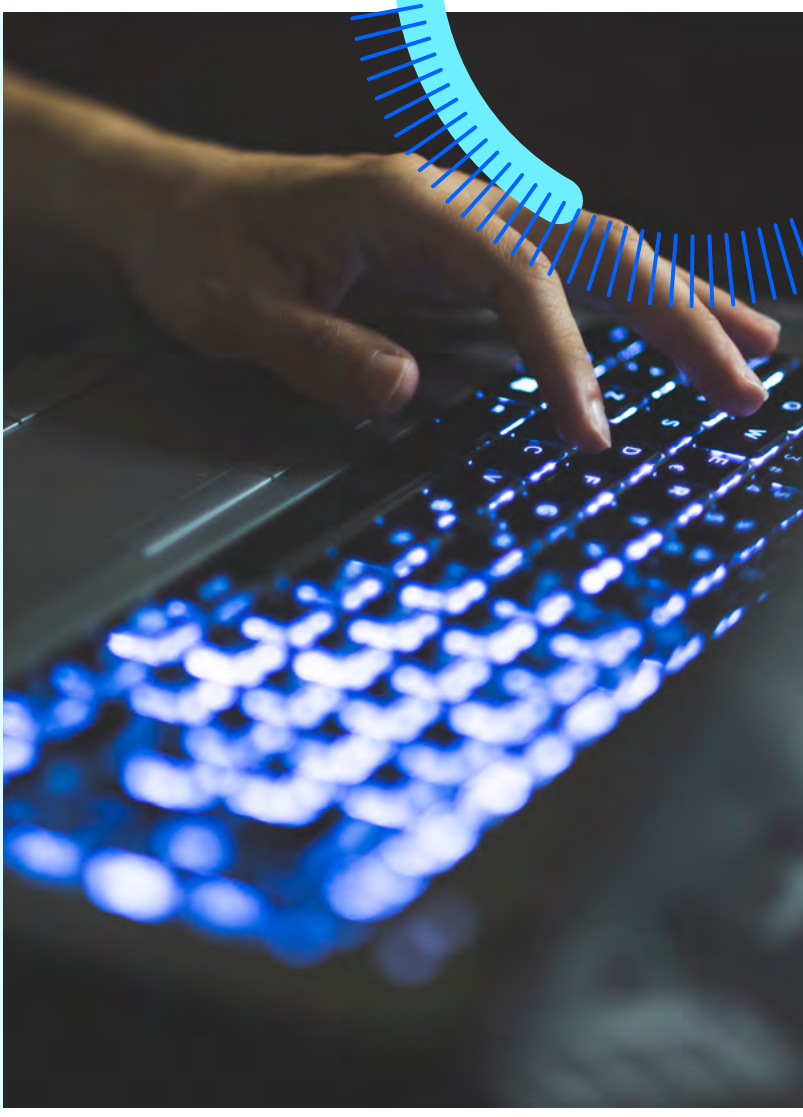
Fraudsters and scammers use key elements of an identity to commit their crimes. Identity fraud can involve stolen identities, synthetic (fabricated) identities, or a mix of both. For example, a synthetic identity can be built using a real Social Security number (SSN) while trying out fake names to test systems' ability to detect the false identity. If not detected, this new identity begins to appear legitimate, enabling other fraudulent behaviors. Identity theft can be used to obtain an insurance policy, take over an existing account, and file fraudulent claims.

A data breach can expose confidential information from millions of individuals. Criminal hackers sell breached data on the dark web. The packaging of batched usernames and passwords makes this fraud particularly accessible across a broad spectrum, from individual actors to well-organized, technically advanced rings. The reward is high, with a single event potentially costing an individual victim, institution, or insurer hundreds of thousands of dollars.

The data used can include names, addresses, dates of birth, phone numbers, SSNs, email addresses, usernames, passwords, payment methods, and other personally identifiable information (PII). Recent research shows some of the most prized information is authentication data connecting usernames and passwords, as people commonly recycle the same username and password combinations for multiple accounts.

In June 2025, 324 alleged scammers were charged in cases of identity theft, particularly the misuse of patient information to file fraudulent insurance claims. The schemes involved $14.6 billion in intended losses.[1]

In July 2025, a Maryland couple was sentenced in a $20 million insurance fraud scheme for identity theft tactics used to falsify insurance applications. He was sentenced to 12 years in prison; she got four.[2]



ATO & Data Mining: A path of least resistance

Cybercriminals often follow the path of least resistance to execute their schemes. Authentic identity data can be compromised across a wide range of digital environments—some breaches make headlines, while others remain hidden. This stolen information becomes fuel for account takeovers, enabling fraud at scale and threatening P&C claims.

Company data breaches

Major breaches have struck Microsoft, LinkedIn, Meta, T-Mobile, Advance Auto Parts, Change Healthcare, HCA Healthcare, Ticketmaster, and even state and federal agencies, among many others in recent years.

Cyber criminals might also mine companies with less sophisticated, less secure systems run by small operators with little to no cybersecurity budget.

For example, a fraudster could steal usernames and passwords from the neighborhood veterinarian's website, a small nonprofit, or a local retailer. These companies might not be the end target but rather a hub of personal information for individuals who may use the same credentials across their insurance and financial accounts.

Search engine optimization (SEO) diversion

SEO diversion tactics, or "SEO poisoning," where fraudsters create fake websites mimicking insurers' sites, are also prevalent.

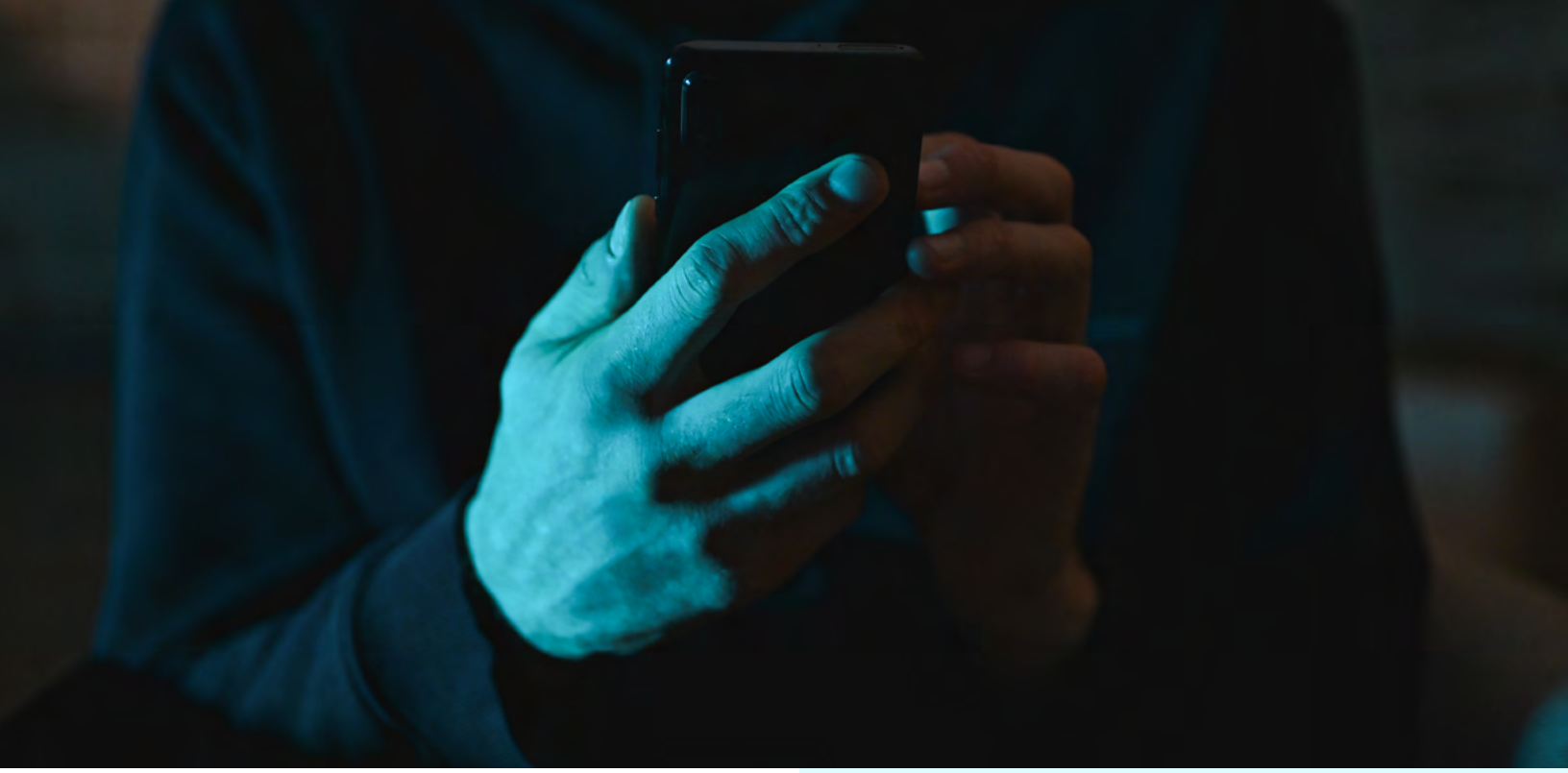
In an SEO scam, a fraudster publishes a spoof website that looks and feels identical to an authentic insurer's website and is optimized to potentially appear at the top of search results for the insurer's brand name—outranking the insurer's actual website. Unsuspecting policyholders use Google, Bing, or another search engine to find their provider's site and visit the fraudulent site instead, where they are lured into providing their usernames and passwords. The policyholder believes they're logging into their account, while the fraudster captures that authentication information and immediately takes over the policyholder's account. Those same fake sites might display an active phone number answered by a real person posing as a company employee, mining data to steal and use elsewhere. While these sites may only exist temporarily, the damage they can cause lasts much longer. A fraudster deploying a fabricated site after a catastrophe has the potential to harvest thousands of credentials quickly, when the insureds are already at a significant disadvantage.

Call Center Spoof

Some insurers have traced security breaches back to their own customer service operations. Fraudsters might call, text, or chat online with a company's customer support team while posing as legitimate policyholders. By manipulating the customer service representative, they succeed in altering account details when they gain unauthorized access and control.

Social Engineering

This scheme refers to fraudsters posing as trusted individuals or entities to manipulate others into divulging confidential information. This scheme continues to evolve and is driven in many instances by highly organized crime rings.



Fraud prevention today goes beyond firewalls and encryption. It also means understanding how scammers play on human emotions. In The Economist's podcast series "Scam Inc," the "Pigs in a Barrel" episode dives into the "Pig Butchering" scam, where fraudsters build trust over time by posing as romantic partners, coworkers, or financial advisors. Their goal? To persuade victims to move money into fake investment platforms. It's a powerful reminder that emotional manipulation is often at the heart of modern scams.[3]

Phishing

Scammers deceive individuals into disclosing confidential login information, known as "phishing." Sometimes, phishing refers specifically to this practice by email, while "vishing" refers to doing so by phone and "smishing" by SMS text message; social media direct messages can be used as well.

SIM swap

This form of identity theft involves a fraudster deceiving a mobile service provider into transferring a victim's phone number to a SIM card the fraudster controls, often after using other social engineering techniques to influence the cellular carrier. Once the switch is made, the attacker can intercept two-factor authentication, reset passwords for hacked accounts, and bypass security protocols. This is also known as SIM hijacking and illustrated in the example.

SIM hijacking illustration

In May 2025, two fraudsters were arrested for trying to steal $200,000 from a Palm Beach, Florida resident. The victim told police someone called him claiming to represent his cell carrier and asking to validate phone numbers using a code sent to him via text message. Shortly after the call, phone numbers connected to the victim's account stopped working. The fraudsters transferred the victim's phone numbers to other cell providers to circumvent two-factor authentication security measures and tried further hacks on the victim's bank account.[4]

Insider threats
Bad actors might infiltrate an organization through employment to access and leverage systems, steal sensitive data, or assist with external cyberattacks.

Password spraying
This relies on users choosing easily guessable passwords such as "12345" or the word "password." Attackers try a set of popular passwords across many accounts.

Credential stuffing
This scam relies on stuffing stolen data into various website portals to see whether victims used the same usernames and passwords across multiple accounts.

Fraudsters can use verified stolen identities to target insurance companies, banks, social media, travel, email accounts, and others. They can hit hundreds of targets across multiple industries, hoping the recycled PII provides access to many more accounts.

In a June 2025 study documented in Cybernews, "researchers found 30 different exposed datasets, each containing anywhere from tens of millions to more than 3.5 billion records. Altogether, they uncovered an overwhelming 16 billion credentials." The login details were mined from many areas, including social media, virtual private networks (VPNs), and developer platforms.[5]

Bot attacks: Validating identities

Automated tool techniques are being used in large-scale attacks. One technique sophisticated fraudsters increasingly use is synthesizing stolen IDs by using bot-driven artificial intelligence (AI) to probe a wide range of potential targets. This method allows the criminal to quickly impersonate real individuals from stolen data, or even to test synthetic IDs for validity.

Bots have been known to attack insurer underwriting and policy application systems to test stolen identities. This might be detected through a significant increase in website hits for a carrier's underwriting platform. A spike of website activity could reveal bots using PII from a known data breach purchased on the dark web. Bots can work through an application for purchase or just the initial underwriting process, disconnecting prior to purchase once the bots exploit an insurer's platform to validate the stolen IDs.

In January 2025, New York regulators fined PayPal $2 million for failing to meet security standards to defend against a 2022 bot attack when cybercriminals used data from a prior breach to target PayPal accounts.[6] Though 35,000 accounts were affected, no unauthorized transactions were initially detected. The validated credentials were likely resold on the dark web for further exploitation. The attackers apparently aimed to identify reused logins across platforms, validating which credentials were still active.

Insurance fraud schemes

The wave of digital deception and cybercriminal activity directly affects the property and casualty industry. Once criminals obtain authentication or login credentials and gain access and control of policyholders' accounts, they typically change account contact information so emails, text messages, and phone calls are routed to the criminal to modify communications and redirect payments to the fraudster. Often, the true policyholder never knows a fraudster has taken over the account and gained control over the policy until it's too late. Here are a few examples of how this information can be used:

Application fraud

Real people's identities are used without their knowledge to apply for insurance. Coverage can be obtained on life, disability, homes, apartments, vehicles, or other property.

Fabricated claims

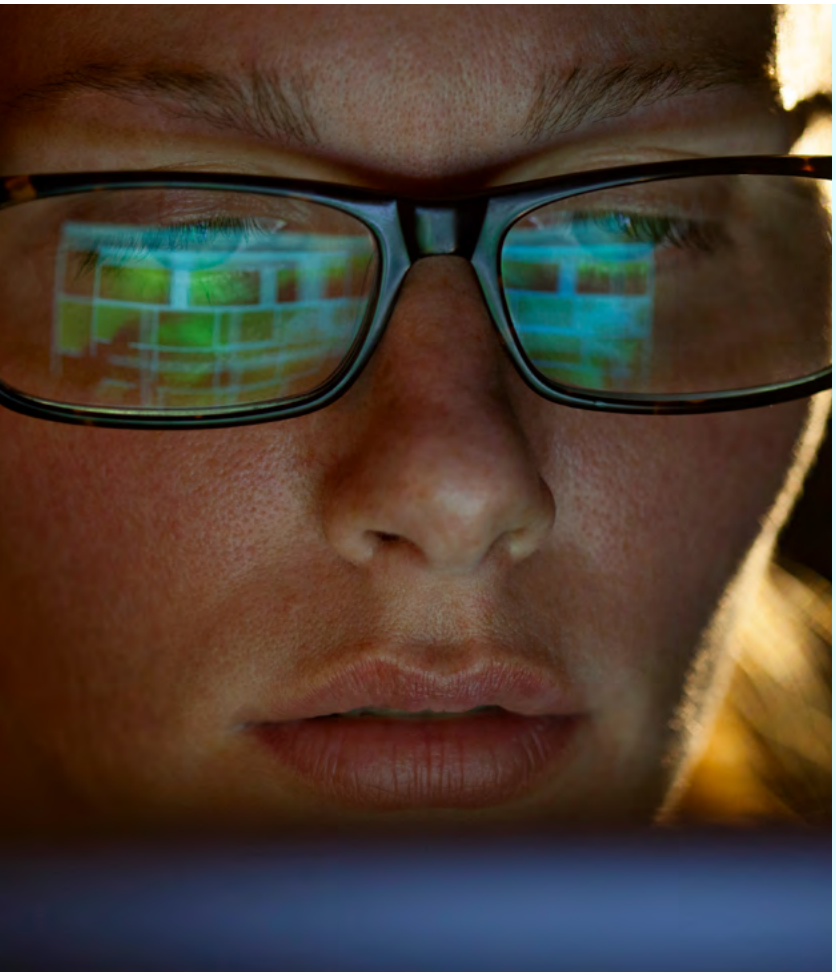
Once fraudsters gain access to unauthorized or fabricated accounts, they submit first-party or third-party claims and fabricate evidence for property damage or injuries incurred or caused, for real or phantom vehicles, for individual claims, or for organized networks and staged accident rings.

Policy manipulation fraud

Exploiting policyholder data is an ever-growing scheme. Fraudsters focus on obtaining an individual's policy details to use the information to impersonate, falsify, and redirect payouts. During the course of the fraud, and depending on the line of business, there might also be a change of beneficiaries, coverages, or deductibles.

Premium prepay/overpay

These schemes are a variation of the cancellation scheme using stolen credit card data. A cybercriminal can use a stolen credit card number to prepay or overpay the policy premiums, then soon after cancel the policy and/or ask for the refund to be issued by check or wire transfer. While the cost of these schemes may seem low on an individual basis, an effective fraudster scaling the operation can quickly drive significant losses for a victim insurer.



Cancellation

Schemes involve canceling a policy early and collecting the refund, which is a feasible scam if the true policyholder prepaid the premiums. When a prepaid policy is canceled mid-term, the insurer will issue a pro-rated refund to the policyholder. Because the policyholder information has been altered, the criminal receives the refund payment.

Verisk case studies

1

In one recent example, a cybercriminal impersonating a policyholder reported a car accident to the victim insurer. The criminal reported striking a person riding a mobility scooter and encouraged the insurer to settle the claim quickly to avoid litigation and increased expense.

- Verisk detected the scheme across multiple carriers because the criminal used the same or similar photographic evidence to substantiate each claim. The photos were generated by AI.
- Verisk's anti-fraud detection programs flagged the suspect photos, prompting additional scrutiny by the carriers.
- Verisk identified that multiple carriers had been attacked within a brief time frame.

2

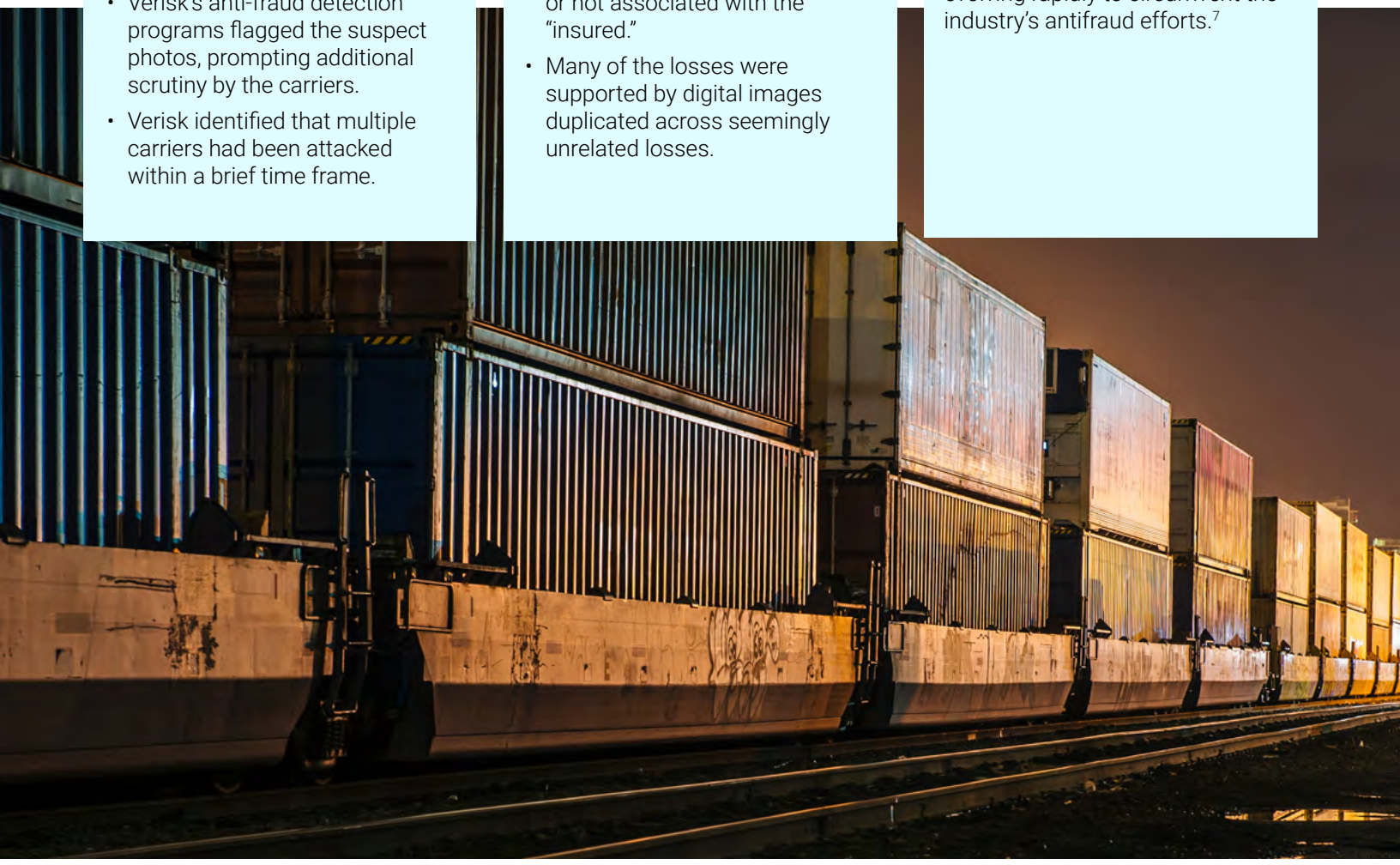
In a separate scenario, the cybercriminal created a variety of identities and secured multiple renter policies before filing online claims for a small fire that damaged home healthcare equipment. The perceived personal tragedy and subsequent health risk often led to prompt payments by insurers. However, several factors pointed to fraud:

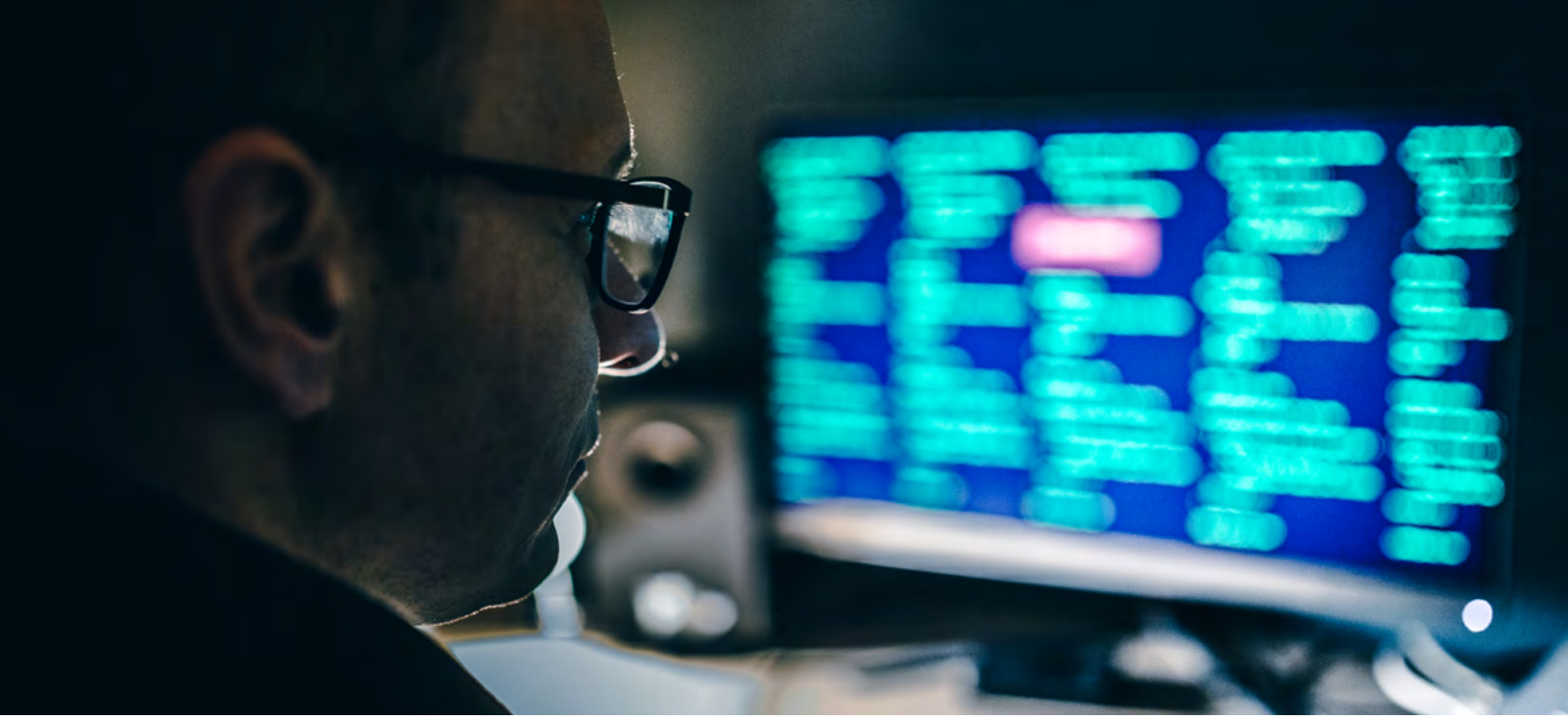
- Most losses were on new policies (often less than 30 days old).
- Many locations were nonexistent or not associated with the "insured."
- Many of the losses were supported by digital images duplicated across seemingly unrelated losses.

3

Commercial lines of business provide fraudsters with high-dollar targets.

Verisk CargoNet® analysts warn of an increase in complex cargo theft schemes involving identity theft and document fraud. Fraudsters are fabricating or stealing IDs to digitally hijack shipments of goods as the transporter or receiver of those goods. These sophisticated operations, which may target supply chains, are often perpetrated by international organized crime groups and are evolving rapidly to circumvent the industry's antifraud efforts.[7]





Top carriers are under attack

ATO fraud has been affecting the life insurance, financial services, retail, and gaming industries for many years. While specific data for the overall impact of identity fraud on the property and casualty industry is limited, broader statistics reflect how the arena is evolving quickly:

The Federal Trade Commission (FTC) reported a significant increase in consumer losses due to fraud, including identity theft and ATO, in 2024. The FTC's Consumer Sentinel Network compiled the data using aggregated reports from consumers and law enforcement agencies. Data indicates that while the number of fraud reports remained stable from 2023 to 2024, the percentage of fraud victims who reported losing money in 2024 was 38%, a double-digit increase compared with 27% in 2023. Of the 6.5 million reports received in 2024, 1.1 million were reports of identity theft.[8]

Top Verisk clients have confirmed ATO is a major concern. It is believed all top carriers are under attack and have been victims of this crime. Many insurers therefore are establishing or enhancing defensive systems to protect their policyholders and their bottom line. Some carriers are using technology to prevent account changes without extra scrutiny. Others are using basic watchlists to spot suspicious traffic associated with certain IP addresses. When ATO schemes are executed at scale, the impact can be significant. Unfortunately, there is no perfect defense.

The FBI's 2024 Internet Crime Report, released in April 2025, indicated the number of identity theft complaints increased 33% from 2023 to 2024. The top three cybercrime categories by complaint volume were phishing/spoofing, extortion, and personal data breaches, which include identity theft and ATO.[9]

Verisk's advice: Securing the future of identity in insurance

As identity fraud continues to evolve, so must insurers' defenses to protect their customers and operations. Effective mitigation requires a **multilayered strategy** that scrutinizes the weakest links in the fraud chain, such as claim documentation and payee data. These elements often serve as the entry points for sophisticated schemes and call for heightened vigilance.

It's critical to use AI-driven fraud detection tools to recognize behavioral metrics, flag anomalies, and map fraud networks. Verisk offers multiple products to support these efforts:

- **Digital Media Forensics** can surface fabricated photos and documents at scale.
- **Network Analysis** can be key for connecting hidden details to surface fabricated evidence or stolen identities and to detect organized crime rings.
- **ClaimSearch®** plays a crucial role in detecting and preventing fraud as a first line of defense, even against new schemes, as Verisk continues to develop additional defenses against these threats.
- **Verisk's RISK:check® Point of Sale** solution offers detection and deterrence at the point of sale, identifying anomalous behavior and patterns of concern.

The growth of self-service platforms has brought greater efficiency—but also new risks. Insurers now face the challenge of delivering convenience to customers while staying compliant and guarding against fraud. Striking this balance requires more than good intentions. It demands close collaboration among insurers, regulators, and technology partners, along with continuous education for both consumers and employees on cybersecurity best practices.

Ultimately, protecting against identity theft is about more than just safeguarding money. It's about maintaining trust by adopting strategies and products that help the insurance industry fight emerging threats. Digital transformation should enhance customer experience, not compromise it.

Sources

1. U.S. Department of Justice, Office of Inspector General. (n.d.). *National health care fraud takedown results in 324 defendants charged in connection with over $1.4 billion in alleged fraud losses.* **https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146**

2. Insurance Journal. (2025, January 27). **https://www.insurancejournal.com/news/east/2025/01/27/809589.htm**

3. The Economist. (2025). Scam Inc. The Intelligence. **https://shows.acast.com/theintelligencepodcast/episodes/scam-inc-1-pigs-in-a-barrel**

4. The Palm Beach Post. (2025, June 2). **https://www.palmbeachpost.com/story/news/crime/2025/06/02/palm-beach-sim-swap-scam/83951380007/**

5. Cybernews. (n.d.). *Billions of credentials exposed: Infostealers data leak.* **https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/**

6. The Record. (2025, January 24). *PayPal fined millions after data breach.* **https://therecord.media/paypal-penalty-millions-data-breach**

7. Franck, T. (2025, May 9). *Cargo thieves attack supply chain* CNBC. **https://www.cnbc.com/2025/05/09/cargo-thieves-attack-supply-chain.html**

8. Federal Trade Commission. (2025, March). *New FTC data show big jump in reported losses to fraud—$12.5 billion in 2024.* **https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024**

9. Federal Bureau of Investigation. (2025, April). *Internet crime report 2024.* FBI & IC3. **https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report**; **https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf**

Verisk