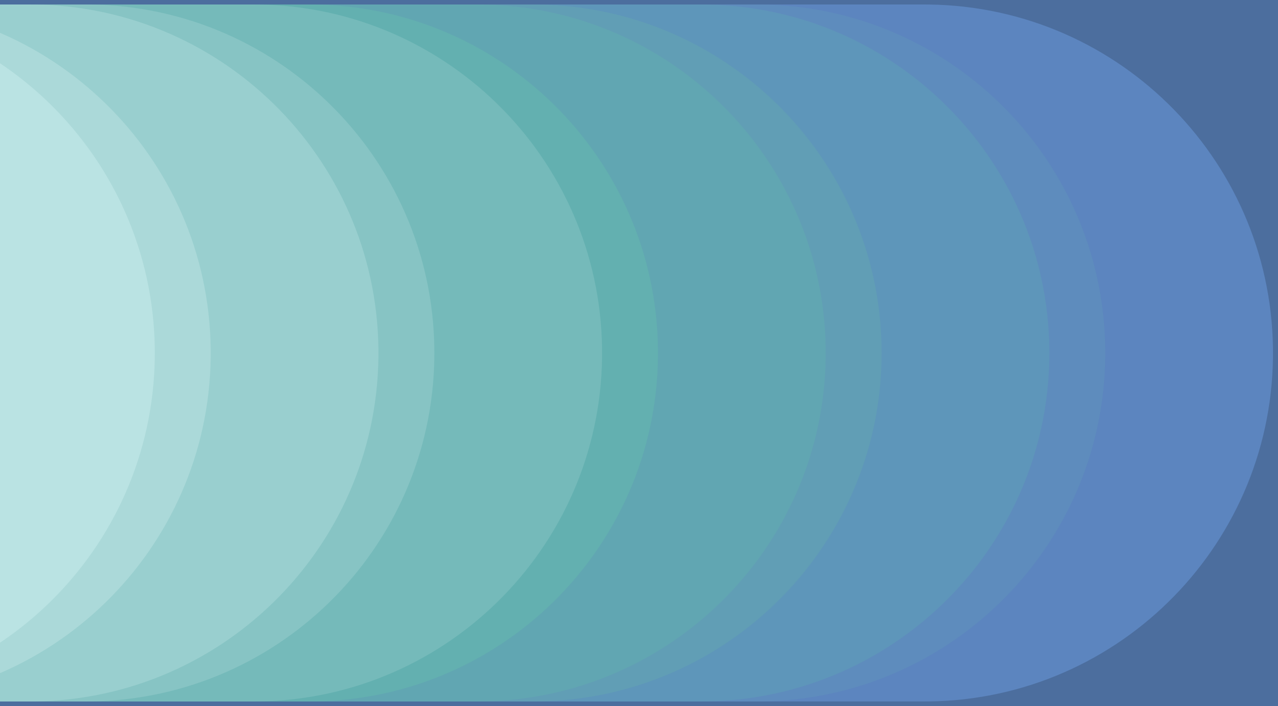
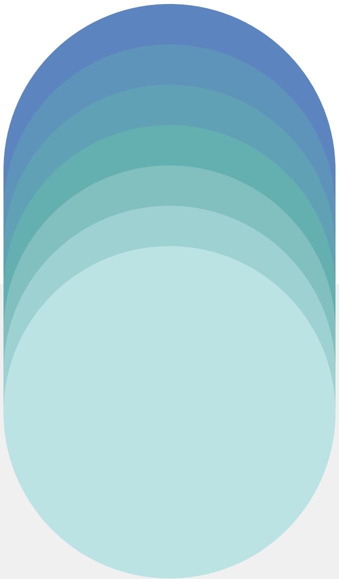
Early Warning®



Three Best Practices for Preventing Synthetic Identity Fraud Losses

GUIDE

Introduction



Synthetic identity fraud in the U.S. is continuing its rapid rise.

> Losses surged from $6 billion in 2016 to $20 billion in 2020[1]—and are expected to surpass $23 billion by 2030[2].

Criminals are flocking to synthetic identity fraud for “good” reason: there's a low barrier to entry, it's difficult to detect and the average payoff is upwards of $81,000[3]. As far as cybercrime goes, it’s a highly lucrative and relatively low risk endeavor.

In this guide, we'll explore common synthetic identity fraud schemes, explain why it's such a troublesome type of fraud—and share best practices for preventing it.

Synthetic identities rely on a stealthy mix of real and fake PII.

A big reason why synthetic identity fraud is so prevalent has to do with a rise in data breaches—and the abundance of personally identifiable information (PII) available to bad actors. Although synthetic identities are fake personas, criminals often use real people's identity credentials to create them.

For example, a criminal might manipulate a real person's identity by **combining real and fabricated PII** (e.g. real name, Social Security number and address with a fake date of birth and phone number).

Or they might **mix the PII of multiple people together**—and possibly throw in some made-up information as well.

And while some synthetic identities are completely fabricated, there's no doubt that access to PII is a big reason synthetic identity fraud is growing.

The shift to digital services across all types of business—which saw a forced acceleration when the COVID-19 pandemic hit—created new opportunities for criminals to breach digital security controls and steal consumers' personal data. Data breaches are a continuing threat. According to a TransUnion report[4], primary data breaches saw a five percent year-over-year increase in 2023—with a person's name and Social Security number being the two most exposed PII elements. The abundance of stolen data available on the dark web has forced prices way down—making it easier than ever for criminals to get their hands on the PII they need to create sophisticated synthetic identities.

Fraudsters use a variety of tactics to profit off synthetic identities.

In the first half of 2023, synthetic identities had access to $994 million[5] in funds from U.S. bank credit cards—a $77 million year-over-year increase.

Before fraudsters can make money off synthetic identities, however, they need to get the identity into the bank's system, typically by opening a new account. Once inside, the next step is gaining access to the FI's funds—by applying for credit cards, lines of credit, loans and other lending services. Three common schemes fraudsters use to establish credit for synthetic identities include:

BUILDING CREDIT FROM SCRATCH

The criminal attempts to open a credit account using a synthetic identity. With no credit history on record, the application will typically be denied. Simply applying for credit, however, automatically creates an initial credit bureau file for the fake identity[6]. To the credit bureaus, the new credit record looks like that of any consumer who hasn't yet built up a credit history, such as young adults and underserved populations. In short, this "rejection" gives the synthetic identity a toe in the door to start opening accounts and building a credit history.

PIGGYBACKING

A fraudster adds the synthetic identity as an authorized user to an unwitting consumer's financial account to legitimize the identity. Piggybacking serves as a springboard from which the synthetic identity can begin building its own positive credit record.

POLLINATION

This ploy is essentially a piggybacking scheme that uses an established synthetic identity to open accounts, and then attaches additional synthetic identities as authorized users. In short, the established synthetic identity "pollinates" multiple new ones.

CLICK HERE TO LEARN MORE

Criminals often nurture synthetic identities for months or even years, making regular payments and behaving like financially responsible consumers. Once satisfied with the credit they've amassed, the criminal will max all credit attached to the identity and abruptly stop making payments. This is called a credit "bust out" because the criminal abandons (or busts out of) the identity and disappears.

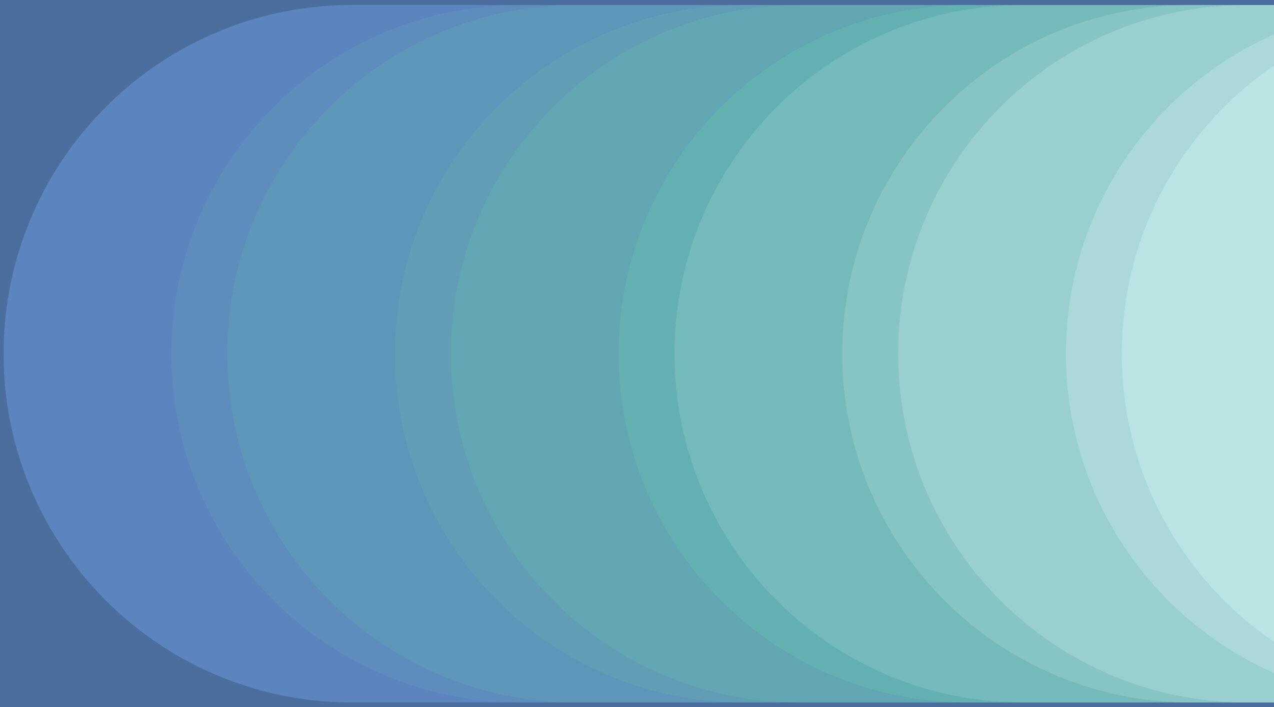
To maximize their profits, organized crime rings sometimes create and use synthetic identities in bulk, building credit for thousands of fake identities simultaneously—then lying in wait until the time is right to bust out. One large crime ring, for example, used 7,000 synthetic identities to amass 25,000 credit cards, resulting in $200 million in losses for banks[7].

CLICK HERE TO LEARN MORE

Synthetic identities are difficult to detect.

Synthetic identity fraud is uniquely hard to detect because **criminals act like regular consumers and are cautious not to raise red flags**—until it's too late. By the time the account defaults, the criminal has made off with the funds.

With true identity theft, the person whose identity is stolen may notice and report the fraud. But with synthetic identity fraud, because the identity is fake, there's no individual victim who can alert the FI.



Preventing synthetic identity fraud requires a proactive approach.

The root cause of growing synthetic identity fraud losses comes down to weaknesses in many account opening and application processes. Traditional risk controls lack the capabilities FIs needed to reliably detect synthetic identities. Here are three best practices that can help:

1

MAKE USE OF SHARED DATABASES

To distinguish between a real and fake identity, FIs need to assess an applicant's PII in context. Consortium data sharing provides FIs with a vast pool of third-party data that looks further back—and dives deeper down—into a person's banking history and behavior, including any changes in personal information like addresses, emails and work history. Because synthetic identities are not attached to real people, this broader, wider view is essential for identifying activities, patterns and other nuanced bits of information that point to potentially synthetic identities.

2

COMPLY WITH KYC REGULATIONS

Identity verification is central to Know Your Customer (KYC) compliance. For good reason: Determining whether a customer really is who they claim to be is a first line of defense against financial fraud of all kinds. In addition to KYC due diligence during onboarding, reducing synthetic identity fraud losses also requires ongoing monitoring once an account is established. Synthetic identity fraud schemes are always evolving. Monitoring adds an extra layer of protection against any synthetic identities that may have slipped by undetected at an earlier stage in the customer relationship (e.g. through a piggybacking or pollination scheme).

3

USE REAL-TIME, PREDICTIVE ANALYTICS

To prevent synthetic identity fraud losses, an FI's identity verification tools must be able to identify whether an applicant's PII has been manipulated and/or manufactured. The solutions FIs have in place should include advanced technologies that can accurately analyze vast amounts of data—in real time—to proactively stop synthetic identities from entering their systems. Verify Identity from Early Warning, for example, analyzes data from thousands of FIs to return an identity confidence risk score—along with a synthetics indicator, which spots and flags potential issues with specific pieces of PII. The service also checks whether an applicant's name, date of birth, and Social Security number matches a legitimate Social Security Administration record[8]. Verify Identity service screened 34M identities and issued 1.1M high-risk alerts in 2023. Because the checks run in the background in real time, FIs can spot high-risk identities at the point of application—without putting valid customers through burdensome identity checks.

TO LEARN MORE ABOUT SYNTHETIC IDENTITY FRAUD TRENDS, READ THE REPORT:

Navigating Synthetic Identity Fraud: Trends, Challenges, and Countermeasures in Banking

References

1 *2021 Synthetic Identity Fraud Report*, FiVerity, October 2021
2 *Biometrics in banking* | Deloitte Insights
3 *2021 Synthetic fraud report*, FiVerity, October 2021
4 *TransUnion Analysis Finds Synthetic Identity Fraud Growing*, TransUnion, August 2023
5 *TransUnion Analysis Finds Synthetic Identity Fraud Growing*, TransUnion, August 2023
6 *Combating synthetic identity fraud*, McKinsey
7 *Combating synthetic identity fraud*, McKinsey
8 Verify SSN does not verify identities, eliminate synthetic identity fraud or reduce fraud. Verify SSN is only available to financial services organizations. Visit earlywarning.com/products to learn more.

ABOUT EARLY WARNING

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial system with cutting-edge fraud and payment solutions for more than three decades. We are also the company behind Zelle®, and the soon-to-launch Paze^{SM}, a wallet that reimagines e-commerce payments. Early Warning partners with more than 2,500 banks and credit unions to increase access to financial services and products and protect financial transactions. Learn more at www.earlywarning.com and connect on LinkedIn.