



5 Steps to Detect and Prevent Synthetic Identity Fraud by Vendors



Table of Contents

The Growth of Synthetic Identity Fraud // 1

How Synthetic Identity Fraud Contributes to Vendor Fraud // 2

How to Detect SIF Using Modern Tools // 4

Preventing Synthetic Identity Fraud // 7

The Growth of Synthetic Identity Fraud and How it Impacts Your Business



Synthetic identity fraud involving vendors and suppliers is a rapidly growing problem for businesses of all kinds. But proactive planning can help prevent it.

↑ **112%**

Increase in
Vendor Fraud



**1 in 5 perpetrators
of external
fraud come from
vendors and
suppliers**

Synthetic identity fraud (SIF) occurs when fraudsters combine personally identifiable information (PII) with fake details to create a fake person or entity. The motive behind using stolen or invented information is personal or financial gain.


SIF can appear in many forms such as loan fraud and transaction fraud. However, it is also prevalent in vendor or procurement fraud. Due to its extensive outreach, SIF resulted in an estimated **\$20 billion in losses** for institutions in recent years. Specifically, ID fraud attacks accounted for **30% of fraud losses**.

This makes it extremely important for businesses to protect themselves against synthetic identity fraud and the severe risks to the table. The security process might seem daunting at first. But adding extra protection to procurement, outsourcing, and vendor onboarding processes can go far in preventing these risks.


Synthetic Identity Fraud Highly Contributes to Vendor Fraud

A typical case of SIF involves the use of accurate information, such as a Social Security number (SSN), along with false details such as a fake name, email address, and postal address. Since this creates whole new identities that have little to no association with scams or fraud incidents, it's tough to spot fraudsters through traditional research and analysis.


This also makes SIF a hotbed for different types of vendor fraud, such as:




Insider Threats




Invoice Fraud



Account Takeover



Kickbacks



Money Laundering



THE ACCELERATING COSTS OF SIF

As the fastest-growing financial crime in recent times, synthetic identity fraud costs affected businesses an average of **\$81,000 to \$97,000 per fraudster**.

While SIF may prey on all types of entities, it often targets financial institutions. Online lenders lose around \$6 billion a year to the fraudsters behind this approach.

Vendor fraud once again stands out as a major contributing factor to these statistics. In a recent study, vendor fraud caused a 112% increase in fraudulent activities such as payment fraud and invoice fraud. According to a global survey for crime and fraud, vendors and suppliers made up **20% of external perpetrators** of fraudulent incidents.

Other types of fraudulent approaches such as procurement fraud and loan fraud also create unsavory challenges for businesses and entities around the globe. In fact, 59% of procurement fraud in the United Kingdom aims at large enterprises and governments, costing them \$120 billion (£89 billion) in total.

 **\$6 Billion**

Annual losses from online lenders to synthetic identity schemes.



This makes SIF and its related risks a global problem. Worldwide instances of vendor fraud and invoice fraud paint a similar picture. For example, 62% of online businesses reported that their experience of global fraud has increased since the start of the COVID-19 pandemic.

SIF also goes beyond transactional and procurement risk factors for commercial entities. If your business falls prey to an illegitimate or fraudulent vendor using synthetic identities, it can also make your customers, trade secrets, and sensitive information more vulnerable to bad actors.

These instances could occur when customers experience data theft, become prone to security risks, and notice a lack in your service quality. As a result, your operations may face the consequences of data loss, customer lawsuits, and loss in revenue. These situations can greatly affect your business's reputation and cause customers and third-party vendor options to second-guess their association with you.

EVERY COMPANY IS A POTENTIAL TARGET.

Even successful, established companies fall prey to vendor fraud schemes.



Invoice Fraud: In 2020, Amazon fell prey to a \$19 million dollar invoice scam, after a pair of fraudsters manipulated Amazon's vendor system to pay for goods the company never purchased or received.

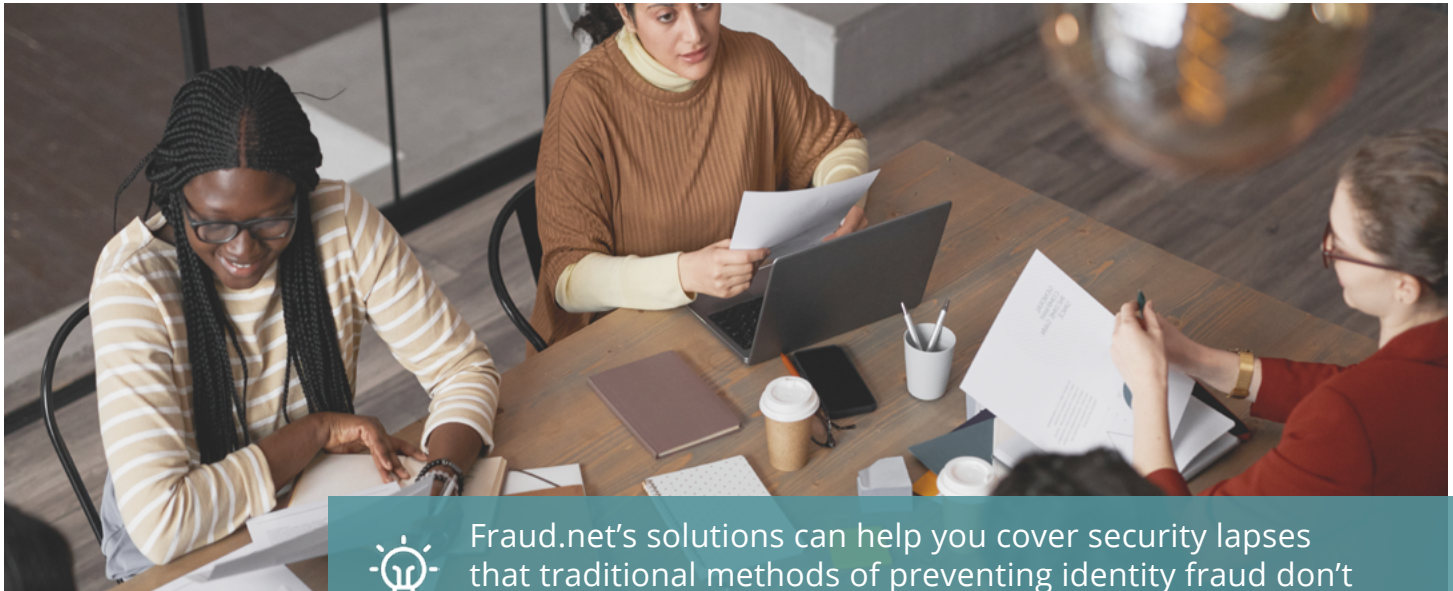


Email Scams: Barbara Corcoran, Shark Tank host, lost \$380,000 to a phishing scam, approving the payment to an email scammer posing as her assistant and requesting payment of a fake invoice appearing to be from a legitimate renovation company.



Loan Fraud: A Kansas State bank reported losing nearly \$200,000 to a fraudster posing as one of their vendors after approving a loan to them.

How to Detect SIF Using Modern Tools



Fraud.net's solutions can help you cover security lapses that traditional methods of preventing identity fraud don't account for.

Considering how people who commit synthetic identity fraud use real and fake information, it can be challenging to detect this type of fraud through many traditional measures. In some cases, fake identities have no prior history of wrongdoing connected to the real-world details associated with them.

Typical supplier selection processes used to include in-person visits and meetings. However, the growing reliance on remote communication has rendered them ineffective for the most part. Basic checks, such as short questionnaires and manual spreadsheets don't do enough to verify business identities and prevent synthetic identity vendor fraud.

This lets many risks, such as procurement and vendor fraud schemes, fall through the cracks. In turn, your business may continue to incur losses until it has lost a significant amount of money and experienced a dent in its reputation.

But how do you look out for fraud committed by identities that have little to no verifiable records in the first place?

Fraud.net's solutions can help you cover security lapses that give way to synthetic identity fraud. By taking advantage of machine learning (ML), artificial intelligence (AI), and modern verification measures, you can steer clear of bad actors that can slip through basic and traditional checks.

This helps you protect your business against various transactional, operational, and reputational risks. As a result, you can save your finances and strengthen your credibility within your target market. You will no longer struggle through invoice fraud and loan or credit card fraud.



You can move forward with this process by following these steps:

01. **USE AUTOMATION FOR ADVANCED ANALYTICS**

Fraud.net's suite of solutions allows you to perform thorough analyses and verification checks promptly through ML and AI-based applications. It enables you to examine common factors such as addresses, and overlooked patterns such as the velocity of a shipping address.

These processes open doors to more stringent checks while also assuring your teams that they are dealing with reliable entities. At the same time, these processes give you peace of mind that you are staying protected against synthetic identity fraud actors, whether they appear as third-party vendors or team members. With advanced analytics and reporting through our dashboards, managing these factors also becomes a walk in the park.

02. **COMBINE APPLICATIONS FOR BETTER WORKFLOW**

By using Fraud.net's application programming interface (API) integrations, you can establish consistent communication between various commonly used platforms and apps. This allows you to carry out your processes seamlessly. It also reduces procurement fraud, vendor fraud, and invoice fraud.

With features such as risk scoring and rules-based decision-making, you can avoid human error and seamlessly put together the results of accurate findings. This helps you prevent miscommunication, resolve bottlenecks and ensure that your activities are performed within a smooth workflow. As a result, you can streamline processes such as procurement and outsourcing.

03. **GET TO KNOW EVERY POTENTIAL VENDOR**

When you have little to no data to identify fraudulent activity from obscure vendors, you may feel like giving them the benefit of the doubt. But that is precisely where SIF can strike. Via Fraud.net's Know-Your-Vendor (KYV) processes, you can learn crucial details about the parties you are about to join hands with.

You can learn about their history with similar transactions by verifying your vendor's details using key parameters, sophisticated tech, and disciplined procedures. This also gives you a way to analyze their submitted information and verify it without jumping through hoops. It goes a long way toward minimizing financial, reputational, and procurement risk factors.



04. **COMPLY WITH AML REGULATIONS**

While operating your business in a world of online fraud, it can be hard to comply with AML regulations. But when you turn to Fraud.net's solutions, it becomes easier for you to design and carry out policies that ensure strict adherence to AML rules that are key to ethical business operations.

This way, you can identify lousy behavior right when you spot it. Besides, this helps you ensure factors such as the respective party's Tax Identification Number (TIN), bank account details, and presence on the terrorist watchlist. You can steer clear of individuals and entities that the government sanctions.

05. **CARRY OUT STRINGENT VENDOR ONBOARDING PROCESSES**

Whether through procurement or outsourcing, verifying your third-party vendor is a crucial process. With the holistic solutions at Fraud.net, you can efficiently perform all verification and analytical activities that show the legitimacy of any parties you might work with.

This step employs application integration and automation through the measures mentioned above. When you combine API keys with systems powered through ML and AI, you can run deeper checks on potential business partners and reduce the risk of dealing with fake vendors.

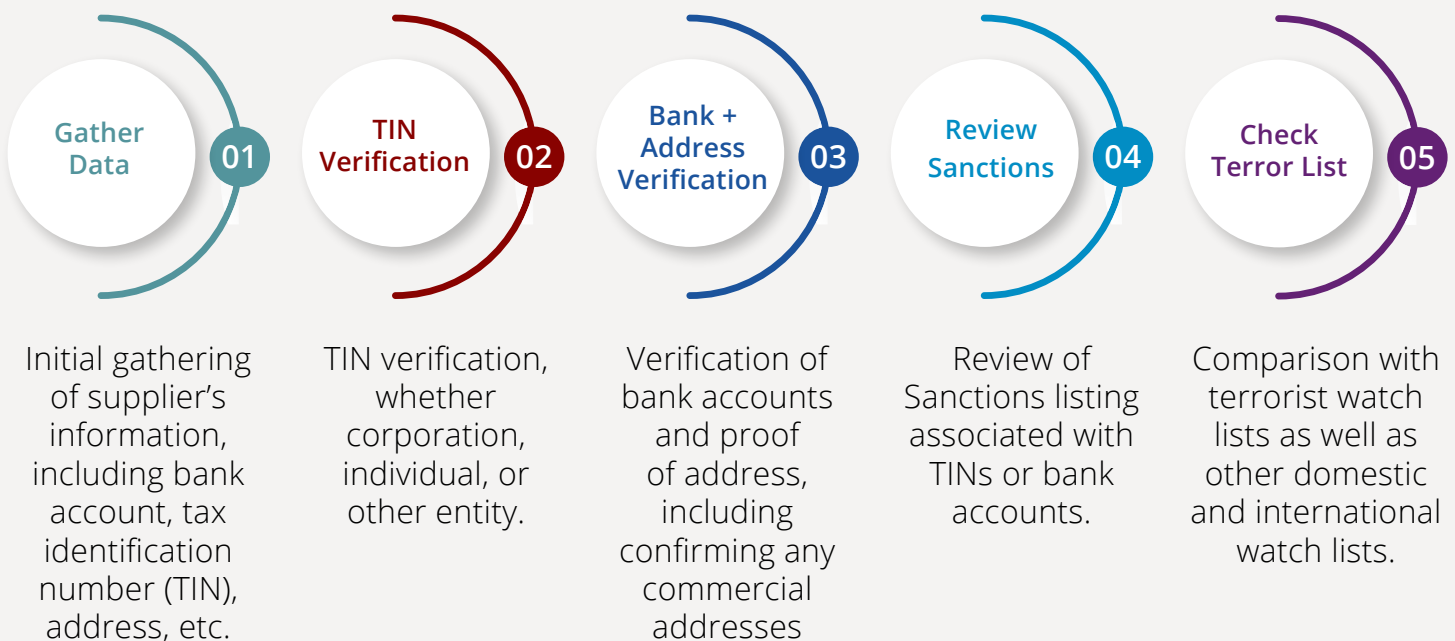
With Fraud.net's modern tools, you can easily accomplish all of these measures through a coherent and comprehensive set of targeted solutions. With our proprietary automated technology that excels at analysis, verification, and compliance, you can reduce your risk of running into bad actors through synthetic identity vendor fraud.

Fraud.net Offers Multiple Checkpoints to Prevent Synthetic Identity Fraud.

As you move forward with preventing procurement fraud, vendor fraud, invoice fraud, and other risks, Fraud.net helps you through multiple points.

RUN EFFECTIVE KYV SOLUTIONS

With our proprietary and AI-powered fraud prevention solution, Fraud.net can assist you with thorough analyses and detailed research on potential vendors. Through a scrupulous Know-Your-Vendor approach, our Application AI executes a swift yet rigorous risk assessment for suppliers, partners, and associates.



This makes it easier to identify red flags and steer clear of bad actors. At the same time, it provides you with a faster turnaround time, prevents human error, and adds to your employee satisfaction by reducing redundant tasks.



Fraud.net's KYV is a five-step process to quickly and accurately de-risk new and existing vendors: Leveraging our powerful **Application AI** product, a leading risk management tool that detects and prevents costly application fraud by leveraging our comprehensive customer verification process, or Know-Your-Customer (KYC), our KYV process can help you fight costly synthetic identity fraud schemes like invoice fraud, insider threats, money laundering, and more.



Fraud.net's proactive, comprehensive solutions let you get a **swift** yet **accurate** overview. This helps your team keep everyone on the same page.

APPROVE TRANSACTIONS BEFORE THEY HAPPEN

After performing deep analyses of your vendors or customers, Fraud.net's AI-powered system also provides you with a final check of factors such as the velocity of shipping addresses and links to previous fraudulent instances.

This allows you to make sure that your transaction with a vendor is free of identity theft. At the same time, it allows you to stay away from evil entities that might not be attempting synthetic identity theft but may very well be a procurement risk for your business.

GET A QUICK OVERVIEW FOR EXECUTIVE LEADERSHIP

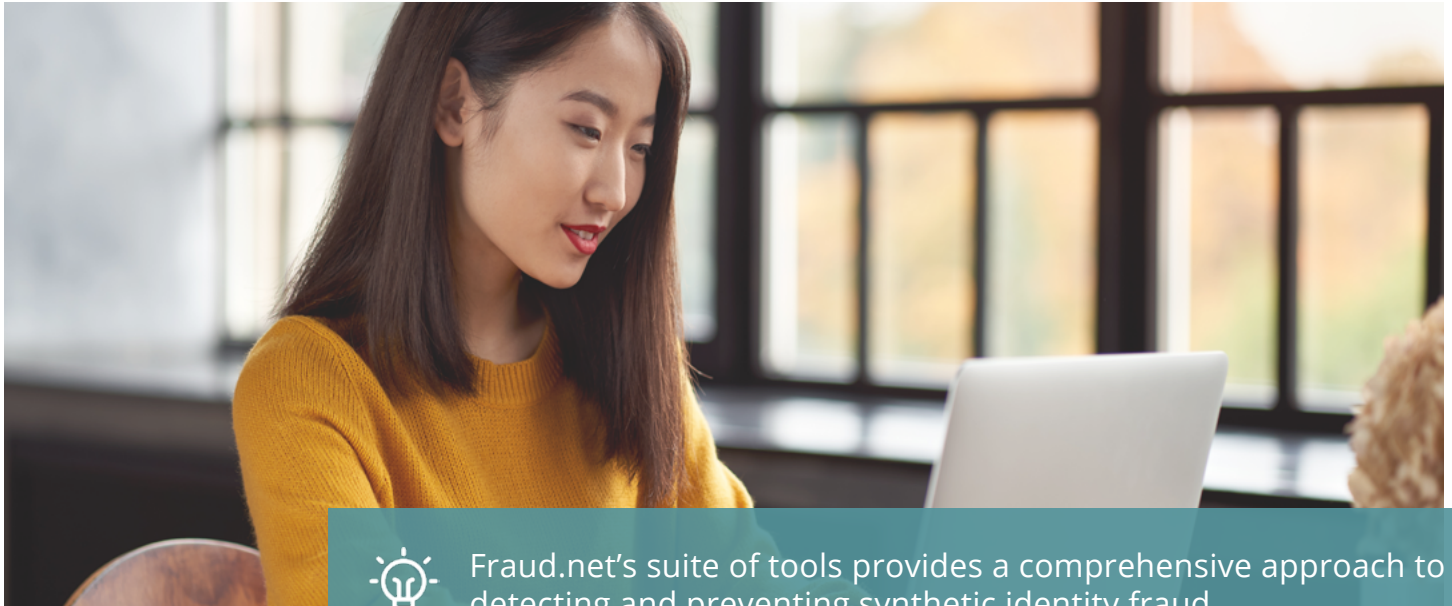
Many processes, such as spreadsheets, hold multiple pressure points for operational teams. In addition to repeatedly entering up-to-date SIF-related data, these systems also require manually prepared reports for executive leadership.

Besides taking more time from staff members who handle procurement, outsourcing or third-party vendor programs, this opens the door to human error in reporting and executive presentation. Fraud.net's solutions let you get a swift yet accurate overview to keep every team level in the loop. This helps your leadership make timely decisions in the light of complex data and customers' behaviors alike.

CONTINUE PERFORMING UP-TO-DATE ANALYSES

Many bad actors could pretend to be a new point of contact from your existing vendor or change the account information for financial or sensitive data transactions. By adhering to evolving policies, you can ensure that you are not falling prey to invoice fraud or procurement risk through SIF.

You can move forward with regular checks of your existing vendors with the help of Fraud.net's automated solutions. They let you track your suppliers and partners using up-to-date procedures while also lightening the load for your procurement and outsourcing staff.



Fraud.net's suite of tools provides a comprehensive approach to detecting and preventing synthetic identity fraud.

PROTECT YOUR INBOX FROM BUSINESS EMAIL COMPROMISE (BEC)

One of the major vectors for vendor fraud is your business email inbox - this is where invoice fraud affected Barbara Corcoran's finances, and where phishing could easily lead to an account takeover and threaten your business payment accounts. Fortunately, Fraud.net's Email AI can help.

Powered by intelligent automation, this email inbox risk scoring tool quickly flags potentially fraudulent emails, such as duplicates or misspelled email addresses. Installing in only minutes, you can quickly de-risk your inbox and prevent vendor fraud - and with each trust/do not trust decision, the tool learns and adjusts its risk scoring for future emails.

ADJUST YOUR VENDOR SCORING ACCORDING TO UPDATES

Whether you are concerned about pricing changes or market conditions, you may need to keep adjusting your vendor score to more clearly reflect each party's credibility. Through Fraud.net, you can easily get a full view of current and potential synthetic identity fraud risks.

In addition to helping you readjust your expectations and trust in each vendor, this process enables you to detect inconsistencies in their behavior. In turn, you can improve your business's resilience against malicious parties. After vendor onboarding, you can adopt this practice as an ongoing process to get the most out of your analyses.

To learn more about how Fraud.net can help protect you against synthetic identity fraud and its risks to your business, don't hesitate to contact our experts and request a KYV demo today.

[REQUEST DEMO](#)