THOMSON REUTERS®

What you need to know about synthetic identity fraud

How to spot and combat new, more sophisticated methods of fraud

What you need to know about synthetic identity fraud

The growth in fraudulent transactions and identity fraud has mushroomed in recent years, and the COVID-19 pandemic has escalated the problem substantially. The pandemic lockdown, combined with the stimulus payments, created a mass rush to online shopping and banking, opening new opportunities for criminals. Many of those over the age of 55 who moved online for the first time were among the most vulnerable to these forms of account and identity fraud.

Financial institutions, who have been early to offer online accounts and digital services, are under increasing pressure to prevent new forms of identity fraud. The revised Customer Due Diligence Rule (CDD Rule) of 2018 strengthened customer verification efforts, requiring covered financial institutions to identify and verify customers and beneficial owners.

Fraudsters, however, are using new methods and technologies to scam banks and individuals, creating believable business and consumer identities that are entirely fictitious. Leaders of fraud prevention efforts have found themselves challenged to effectively identify and counter these new forms of fraud.

Fraudsters are using new methods and technologies to scam banks and individuals.

Why synthetic identity fraud is so dangerous

Synthetic identity fraud is one of the fastest growing financial crimes in the U.S. and is of increasing concern to regulators. Current estimates show that synthetic identity fraud has already cost U.S. lenders nearly $6 billion, with that number expected to climb.

Not an appropriation of another's identity, synthetic identity fraud is the creation of an entirely new fictitious identity. The synthetic identity is cobbled together from stolen personal identifying information and developed over time. Because of the patience with which fraudsters go about establishing an identity and baseline credit history, this type of fraud can go undetected for a long time. The synthetic identities combine valid with fictitious information making this fraud even more difficult to unravel.

Synthetic identity fraud has already cost U.S. lenders nearly $6 billion.

Understand identity fraud by type

To grapple with this growing problem, it's helpful to understand it in context of other types of account and identity fraud.

Identity theft

Identity theft is exactly what the name implies. Someone steals another party's personal information and then uses it to fraudulently establish other financial accounts under that name. Particularly vulnerable to identity theft are seniors and children who may not know about the theft until they are adults. Identity theft can be facilitated by the theft of someone's outgoing mail or by securing another's personal identifying information.

Someone steals another party's personal information and then uses it to fraudulently establish other financial accounts under that name.

Account takeover fraud

In account takeovers, a fraudster accesses another's account, changes key information, and then makes transactions using the account. In essence, it is a combination of identity theft and fraud. An account takeover might happen in scenarios like the following:

In some cases, malware is installed on a person's computer or mobile device, allowing the thief to steal login credentials or personal information. These credentials and personal information are sold on the dark web. A buyer tests the credentials and if gaining access, begins to lock out the legitimate account owner and control the account.

In other cases, fraudsters buy stolen credentials on the dark web and then use computer programs, or bots, to automate mass logins and gain access to accounts.

Synthetic identity fraud

Perhaps the most recent form of identity fraud, synthetic identity fraud, is enabled by the creation of an entirely new fictitious identity. Unlike a traditional identity theft, synthetic identities are compiled from various, separately collected elements of personal identifiable information.

Creation of a new fake identity might follow a process like this:

A fraudster purchases personal information, which is offered for sale on the dark web. (Most of this information is gleaned from data breaches. Financial institutions and other companies that collect personal information are common victims of such breaches.)

Fraud can be enabled by the creation of an entirely new fictitious identity.

Starting with a single piece of legitimate personal information, such as a Social Security number or a business taxpayer ID, a fraudster creates a new “synthetic” identity and applies for a credit card or creates an online retail account.

Playing the long game, the fraudster makes small purchases and pays them off quickly, establishing a credit history. It’s not uncommon for fake social media accounts to be created to support the fiction. It’s also not uncommon for this credit history building to take place slowly, over the course of a year or two.

Having created an identity trail that looks like one belonging to a real person or company, the fraudster opens other, larger credit lines then maxes out the credit available before abandoning the identity and moving on. The most sophisticated fraudsters can create and manage multiple fake personas at once.

A fraudster creates a new “synthetic” identity and applies for a credit card or creates an online retail account.

How the financial industry is reacting to synthetic identity fraud

In May 2021, the Federal Reserve published a formal definition of synthetic identity fraud, developed by a group of fraud experts:

"The use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain."

Included with this definition is a description of identifiers used in creating a synthetic identity, categorized as "primary" and "supplemental" elements. Primary elements are considered typically unique to an individual or profile, such as a combination of name, date of birth, Social Security number, and other government-issued identifiers.

Supplemental elements used in synthetic identity fraud include information that cannot in itself establish an identity but that is often used to support its validity. Typical examples include mailing addresses, phone numbers, email addresses, or a digital footprint.

The Fed hopes this definition will lead to changes in the way financial organizations go about identifying synthetic identity fraud and categorizing and responding to it properly when it occurs.

So, how do you identify synthetic identities?

In verifying an identity, it's no longer as straightforward as requesting multiple forms of identification, as the risk that such identification is fraudulent is growing. Organizations must understand these new risks, know where to look for answers, and adjust their fraud-prevention processes.

Conventional fraud detection models can miss synthetic identities because fraudster accounts appear legitimate. Rather than discarding existing fraud prevention methods, experts recommend keeping the existing foundation in place while augmenting it with new security measures.

Implement powerful technology for identity fraud prevention

Investigators should assume that every identity is potentially false and act accordingly, experts advise. They should consider whether they have access to a full repository of public records to validate that their subject's full data exists in multiple data sets, such as in all three credit bureaus, in utility files, in work records, in bank account records, to name just a few examples of sources evaluated by businesses doing identity checks today.

Investigators should assess whether they are gathering enough personally identifiable information to fully validate that the subject exists in records. It's not enough to have just a subject's name and date of birth. Searches should produce their phone number, address, email information, etc.

To uncover whether their subject is a newly created identity, researchers should try to discover how long the subject's identity has existed in the records. They should check whether searches on the subject turn up similar identities in public record databases. In reviewing search results, investigators should look for signs suggesting that the subject person or business was manufactured.

Simply put, as artificial intelligence technology and tools grow more sophisticated in performing identity verification and know your customer checks, compliance professionals today should take advantage of the power they offer to dig deeper, deliver up-to-date data, and weed out irrelevant findings.

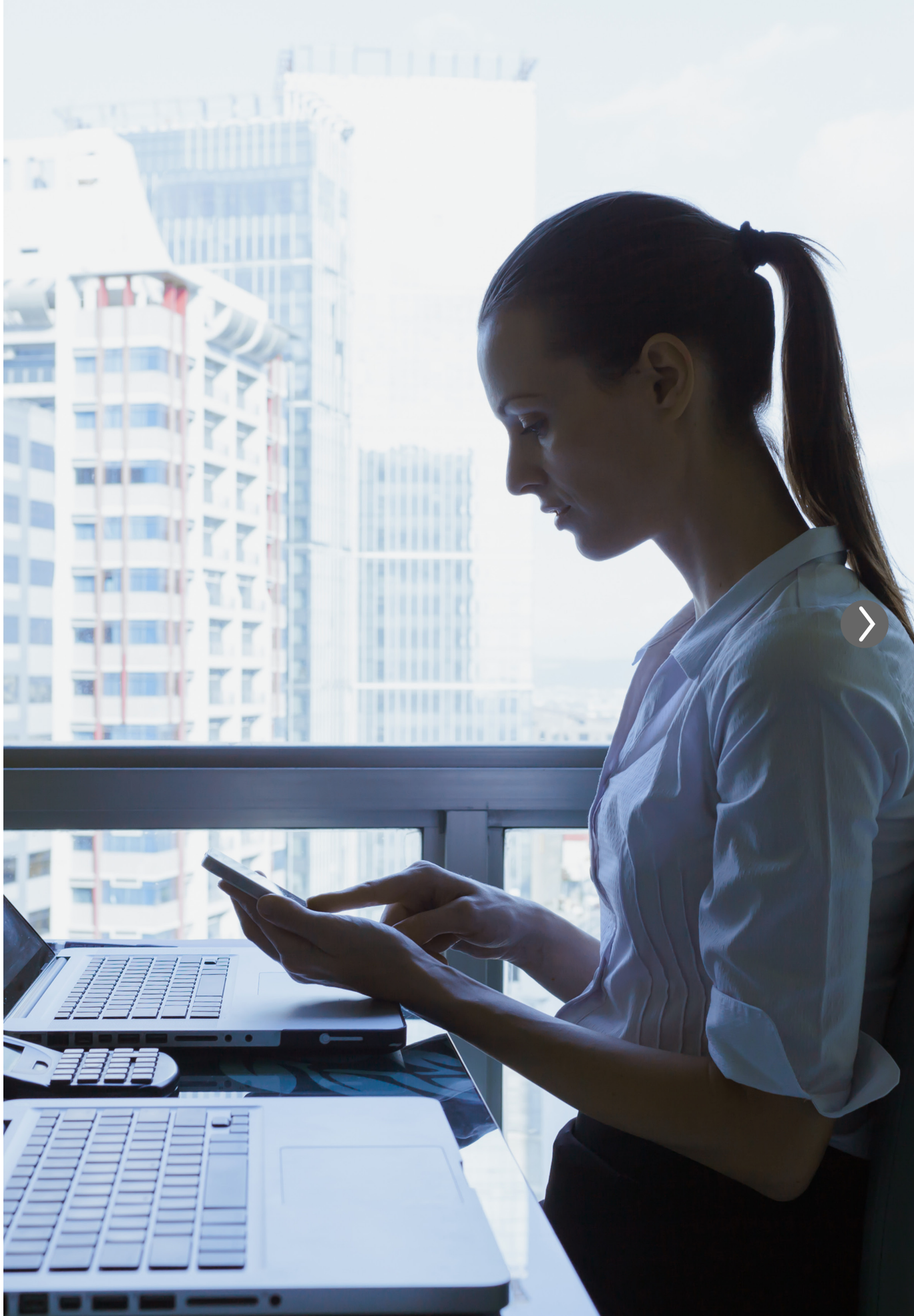
Enhance know-your-customer processes

Gaps in know-your-customer (KYC) processes can allow instances of identity fraud to slip through. Even the toughest, most documented KYC process must rely on human beings to carry them out. No matter how well-written the policy, individual human judgment is required at several steps along the way.

In evaluating your KYC processes, take a careful look at how these functions are structured:

- Do KYC employees feel less valued than front-office workers? If yes, their motivation to pursue investigations diligently and dig deeply will suffer.
- Do these employees have enough time to complete their work? If not, thoroughness will be compromised.
- Are adequate tools in place for them to conduct thorough electronic identity verification research? Public records information technology enhanced with advanced data analytics can boost accuracy and efficiency.

This technology allows investigators to compare information provided by the potential client against public and proprietary records data, rapidly indicating matches and flagging any redundant information or factors for further research. Drawing on multitudes of data points, these tools can also indicate whether there are multiple confirming data sources for the findings and reveal the underlying source material.



Thomson Reuters® CLEAR, the risk investigation and mitigation solution, provides the information you need to quickly and confidently confirm identities and monitor and anticipate risk:

CLEAR ID Confirm: Locate, identify, and connect the facts you need to confirm whether an identity is valid.

CLEAR Risk Inform: Get immediate risk insights for individuals and businesses in just one search.

CLEAR EDD: Understand who you are really doing business with.

CLEAR Adverse Media: Protect your reputation by revealing sources of adverse news and media.

tr.com/clear

THOMSON REUTERS®