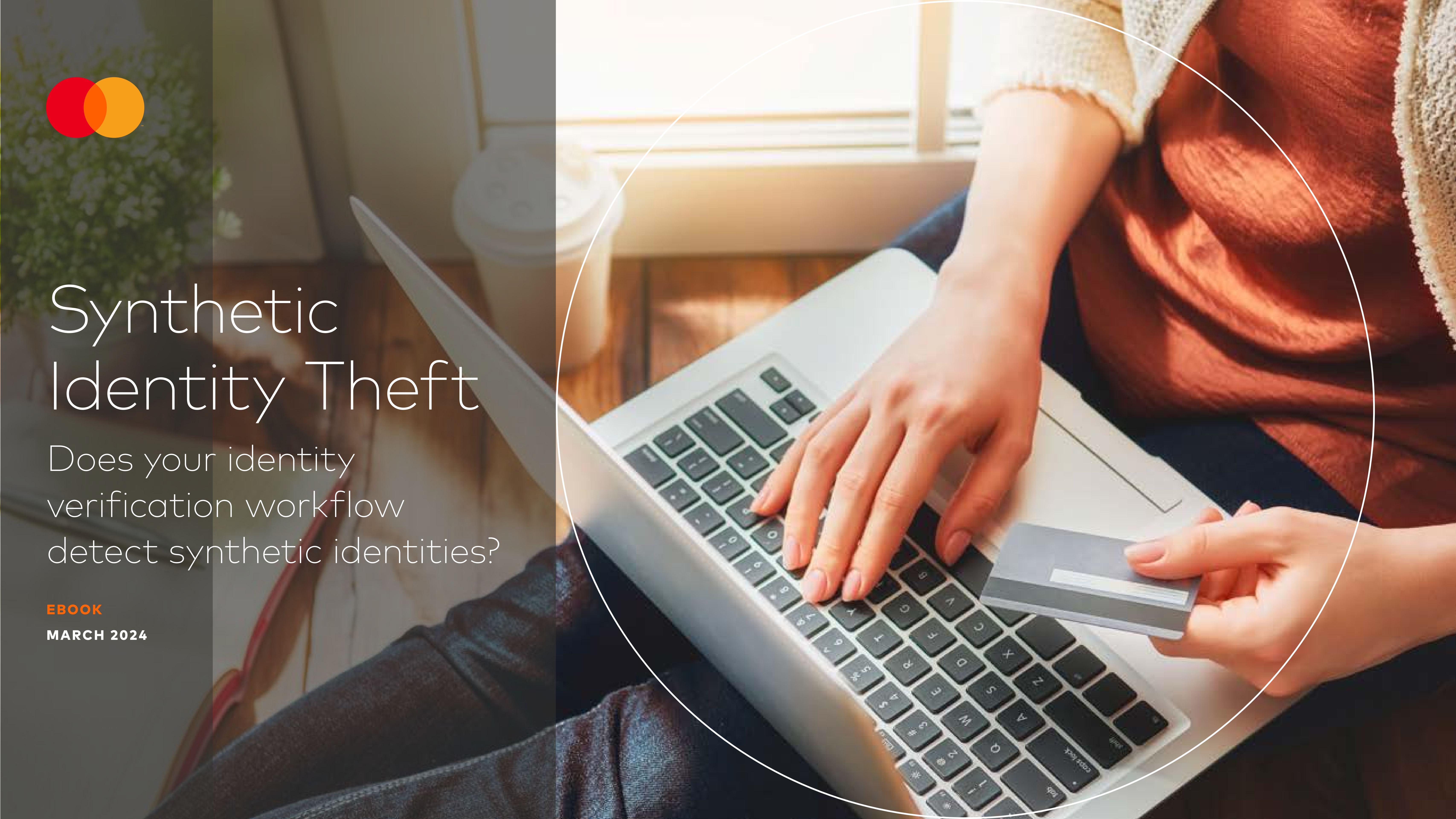


Synthetic Identity Theft

Does your identity verification workflow detect synthetic identities?

EBOOK

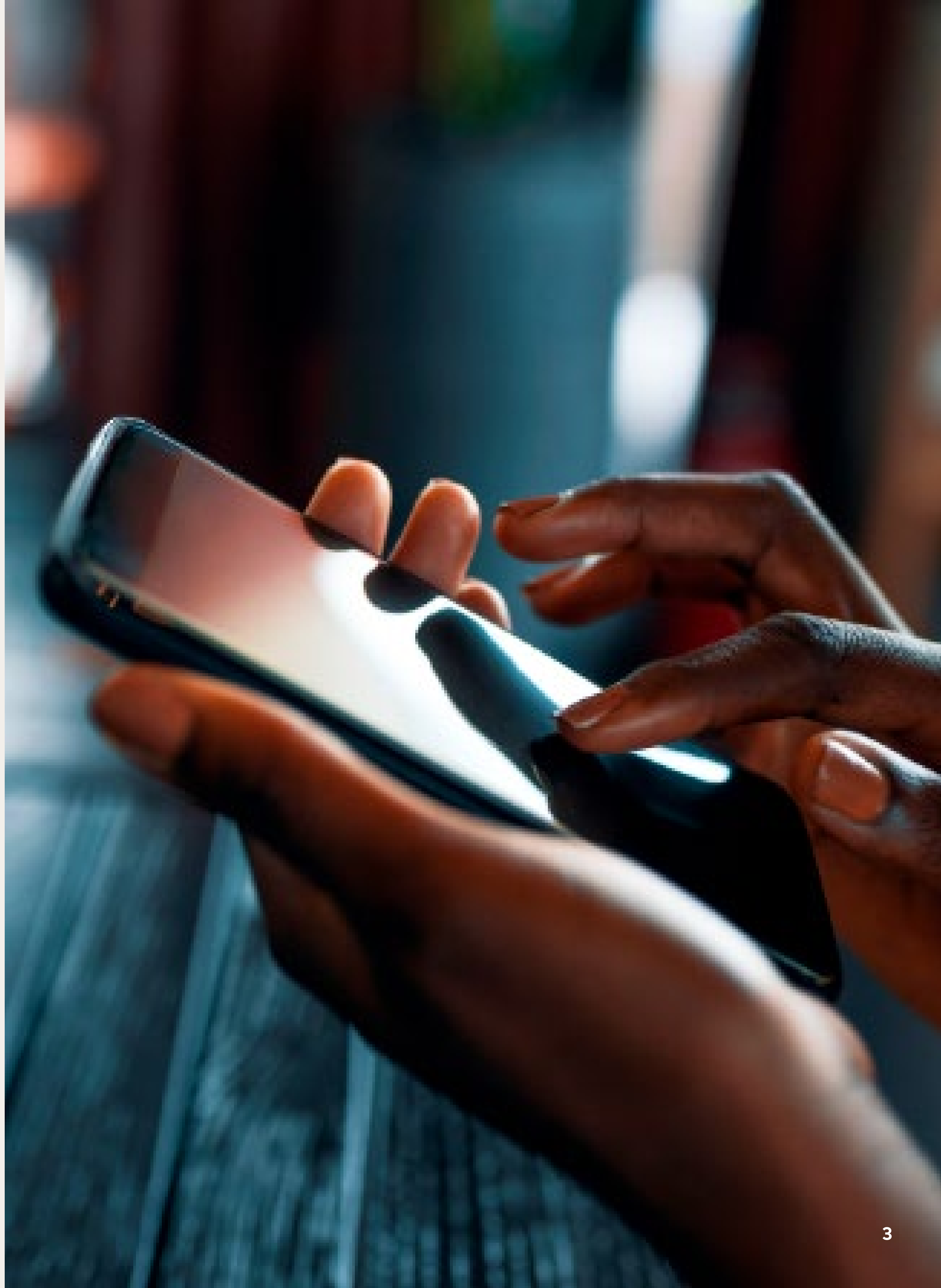
MARCH 2024

Contents

Discover how this fast-growing crime threatens every business and why you need to update your toolkit - today

Synthetic identity theft is a crime perpetrated by bad actors using real and fake personal information to craft an authentic looking digital identity. This type of fraud has surpassed credit card fraud and identity theft as the fastest-growing crime in the world.[1] In fact, according to TransUnion,[2] synthetic identity fraud was up 132% globally in 2022, with 46% of global organizations having experienced the crime that year.[3]

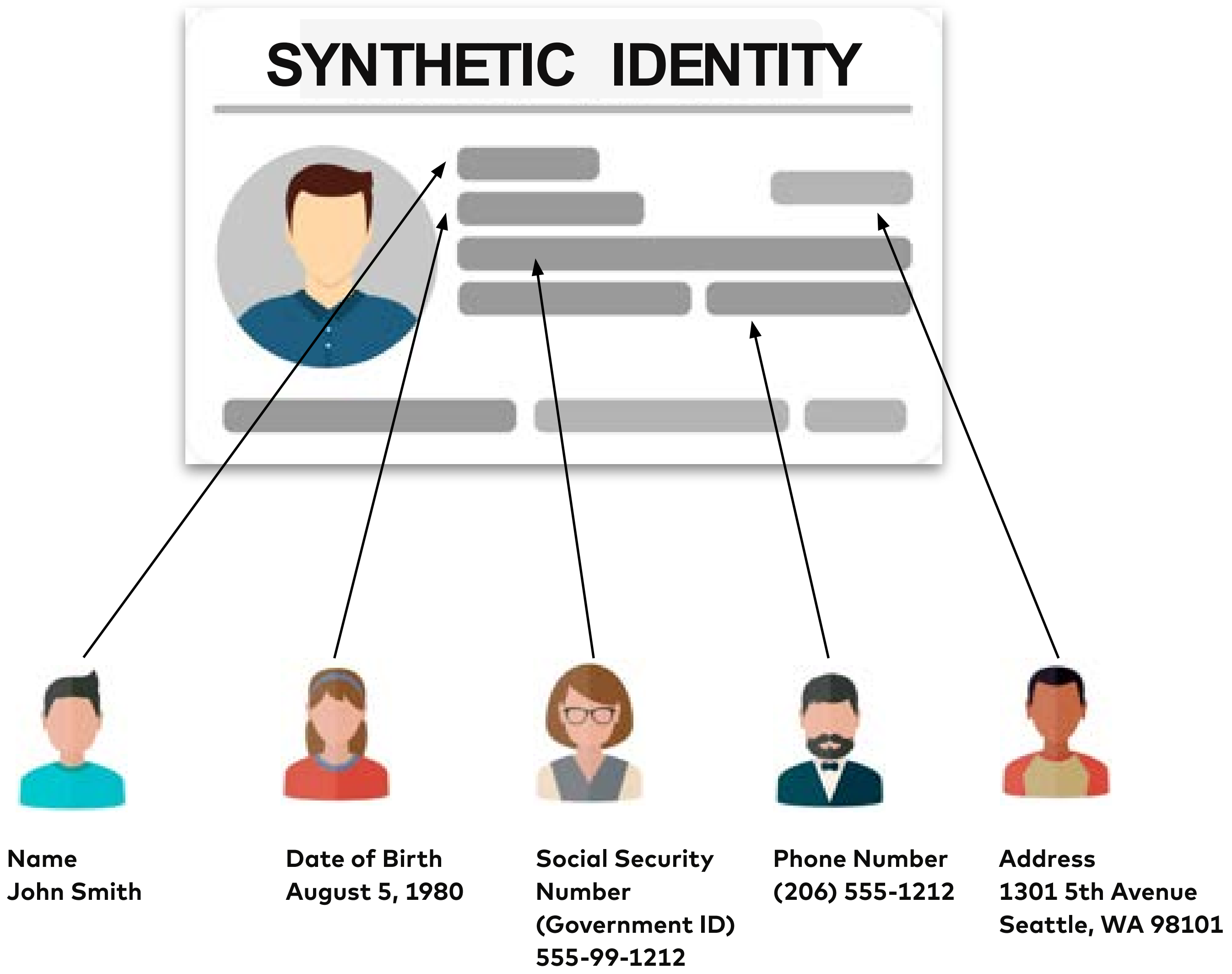
The problem? Personal identity information exposed from data breaches often winds up for sale on dark web marketplaces. This enables fraudsters to easily purchase the data they require to commit synthetic identity fraud.



1. Trends in synthetic identity fraud, Thompson Reuters, 2023
2. 2023 State of Omnichannel Fraud Report, TransUnion, 2023
3. 46 percent of organizations faced synthetic identity fraud in 2022, Security Magazine, 2023

What is synthetic identity theft?

Synthetic identity theft occurs when a bad actor uses a composite of personal information from several people to create an authentic-looking identity. This person may also use fabricated personal information to manufacture the identity. Personal information used may include name, national identification number (NIN), birth date and home address. For example, in the US, a fraudster might use a stolen Social Security number along with the personal information of multiple people — such as email address, home address and birth date to form a new identity. Similarly, in the UK, a stolen NIN from one person and a home address from another may be used to form a fictitious profile. When the attributes are combined, the identities may appear legitimate given that parts of the whole are real.



Name
John Smith

Date of Birth
August 5, 1980

Social Security
Number
(Government ID)
555-99-1212

Phone Number
(206) 555-1212

Address
1301 5th Avenue
Seattle, WA 98101

This is why synthetic identity theft is so difficult to detect

1

Sophisticated fraudsters playing the long game

Synthetic identity fraudsters are patient. enough to carry out long-term, large-scale fraud. They can take months, even years to nurture an identity and establish the integrity of its profiles to achieve sustained credibility. In 2019, McKinsey & Company[4] reported that in the US alone, synthetic fraud accounted for 10%–15% of charge-offs in a typical unsecured lending portfolio. An Aite Group[5] report estimated that synthetic identity fraud for unsecured credit products will surpass US$2.4 billion in 2023. Further, the Deloitte Center for Financial Services expects synthetic identity fraud to generate at least US$23 billion in losses by 2030.[6]

Some synthetic identities include real personal information with the addition of a stolen government-issued identification number. This makes detection even more difficult, as some countries do not have an easy way to validate these unique identification numbers.

2

The youngest victims

In the US, fraudsters often steal the Social Security numbers of children. In fact, according to 2021 study by Javelin,[7] identity theft affects 1.25 million children – or approximately one out of 50 children – every year. Most children do not have a credit history, so bad actors use their identifiers as a “fresh start.” A bad actor can use the child’s credentials for years without detection. Most victims are unaware of identity theft until they turn 18 and apply for credit cards or student loans.

Typically, when a person’s identity is compromised, the first sign is a complaint or concern raised by that person. However, if the person whose identity has been synthetized is a child without personal financial accounts, there’s no way to notice and flag fraudulent activity.

[4] Fighting back against synthetic identity fraud, McKinsey & Company, 2019Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise, Aite, 2021

[5] Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise, Aite, 2021

[6] Deloitte Center for Financial Services analysis of data from Auriemma Group and the 2022 Federal Reserve Payments Study

[7] Child Identity Fraud: A web of deception and loss, Javelin, 2021

3

Fraudsters are good actors

Fraudsters operate as wolves, insisting they're sheep. When their identities are questioned, they become incensed, insisting they're the good customer they pretend to be. If they're able to convince the merchant their transaction was falsely declined, the interaction becomes a further reason for trust and credibility. And remember, these are patient criminals who take extra care to maintain synthetic identities with strong credit scores.

For example, in the US, a bad actor might spend years building a high FICO score. In Germany, a fraudster might spend time building a good SCHUFA score. A credit application is more likely to pass underwriting checks if the applicant has excellent credit. While it may seem to be more trouble than it is worth, for fraudsters who are well versed in the field, it's an investment. Fraudsters often use automated tools such as bots to quickly create hundreds, sometimes thousands, of online accounts or to submit online applications. To evade detection, they may also use device emulators to reset device IDs and mimic behaviors of good consumers.

4

Traditional methods and today's synthetic identity fraudster

Traditional fraud tools that were designed to capture stolen identity activities do not serve well in solving synthetic identity crime. With stolen identity information, traditional fraudsters act quickly to impersonate the owner and capitalize on the opportunity. Synthetic identity fraudsters, on the other hand, behave quite differently, taking the time and energy to curate a profile before acting on it. Because of these differences, their detected behaviors lead to different risk signals. They exhibit different characteristics when they are translated into data attributes.

Data inconsistencies — such as identity elements not matching with reality — are strong signals for both stolen and synthetic identities. For example, a relative increase in usage velocity of an identity is a strong signal for the case of stolen identity fraud. This is because regular fraudsters tend to use stolen identities as soon as possible. However, that is not the case for synthetic identities. Similarly, while historical fraud blacklists have been moderate indicators for stolen identities, they are not strong indicators for synthetic fraud as the identities have not traditionally been flagged as bad.

How fraudsters use synthetic identities

Banking and lending

Synthetic fraudsters often employ credit busts or bust-out fraud, in which a fraudster or fraud ring applies for many credit cards or bank loans using one or more synthetic identities.

The fraudsters then incubate these accounts for months, sometimes years, to build good credit. As their credit improves, they take out as many lines of credit as possible from different lenders. When the time is right, like farmers reaping a crop, the fraudsters bust out, maxing out all the credit lines at once or within a short time frame.

To the lenders, the accounts looked legitimate the entire time because they were in good standing and exhibited authentic-looking activity. With tactics like these, synthetic identity theft costs lenders billions; with losses in the US alone estimated to have been US$20 billion in 2020.[8]

[8] 2021 Identity Fraud Report, FiVerity, 2021

Online marketplaces and e-commerce

Some fraudsters target online marketplaces to commit triangulation fraud. Triangulation fraud is an elaborate scheme that involves three parties: a fraudster, a legitimate merchant and an unsuspecting customer.

First, the fraudster uses a synthetic identity to open an account on an online marketplace and sets up a store front. Next, they buy products from legitimate merchants using stolen credit cards or cards they obtained with synthetic identities. Finally, the fraudster sells the products on the online marketplace.

Buyers have no idea that they've purchased products from a fraudster engaging in triangulation fraud. Worse still, the suppliers to the fraudulent merchants are hit with chargebacks because of the invalid credit cards.

Credit repair services

Fraudsters sometimes scam consumers by masquerading as credit repair companies. They charge a fee to fix a consumer's bad credit. However, instead of helping consumers improve their credit using legitimate means, the fraudsters provide them step-by-step instructions on how to commit identity theft.

The instructions are lengthy and include steps such as getting a Credit Protection Number (CPN) with a fake SSN, getting a new phone number and email address and selecting a new home address. The final steps include applying for credit to establish a new credit file and buying tradelines. These credit repair companies are actually synthetic identity farms in disguise and harm the consumers who use them.

How to battle synthetic identity theft

Fighting synthetic identity thieves can be like playing chess; they think three steps ahead so you must think four steps ahead to counter the move. One piece of information that fraudsters depend on for successful synthetic identities is unique identifiers, whether it be a Social Security number or an NIN. These identifiers can be purchased or stolen, which is relatively easy.

A static identification attribute that does not change over time is useful for synthetic fraud. This is because once the fraudsters have it, they can use it until they're caught - without fear of it changing.

Some companies leverage these static identity attributes to verify identities and that is, in part, their shortfall. Why? These identifiers alone are vulnerable due to their static nature. This means that while some banks and merchants use risk-assessment tools that apply rules-based algorithms to these static attributes, it is not enough as fraudsters grow more sophisticated by the day.

Tracking the digital footprint

At Mastercard Identity, we see digital identity as a complex set of attributes. Consider a DNA analogy: the identity of every person can be traced back to their DNA. You leave a DNA footprint wherever you go and someone can look at that information and come up with a pretty accurate picture of who you are, without ever interacting with you in person. The same goes for digital identity.

Our identity validation process uses core identity elements, considered the global standard for identity verification. These dynamic identity attributes are attributes that can change, but usually not often: name, phone number, email address, home address and IP address.

How to understand synthetic identities

Identifying behaviors

Synthetic fraudsters often employ credit busts or bust-out fraud, in which a Synthetic identities behave differently than other types of stolen identities and generate different types of risk signals. Indicators are the relationship between a synthetic identity's name and email or name and phone number may only exist once, as those attributes are recycled and used in other identities. This is how the use and observations of dynamic identity attributes can help detect synthetic identities.

8. 2021 Identity Fraud Report, FiVerity, 2021

Dynamic attributes

Unlike a static attribute — such as a Social Security number that is country-specific and usually based on one key unique parameter — dynamic attributes are global and can leverage multiple dynamic linkages, metadata, history and activity patterns to validate a user. These attributes are commonly used to verify legitimate identities, which means they are also relevant in assessing synthetic identities. The big difference is how the importance of each signal changes.

For example, the link between identity elements matters a lot more for synthetic identities because there is likely low consistency between elements. With metadata, looking at address history versus the length of credit history is a useful indicator because the duration should be similar. Finally, behavior elements have lots of strong indicators.

IP risk is particularly effective to detect the origination and location of an identity. The bottom line is that these elements can help identify good thin-file customers as well as high-risk customers using synthetic identities.

Risk assessment

Based on what the customer has entered in a record — whether it be an account opening application or a transaction — the information (name, email, phone number and address) can be evaluated. The results rely on probabilistic risk assessment and can provide predictive signals of potential fraud by validating dynamic attributes and how they are linked.

Probabilistic risk assessment reveals patterns of future behavior

Mastercard Identity's approach to identity verification leverages the power of probabilistic risk assessment. Specifically, Mastercard has built two differentiated data sets around five core elements: name, phone number, email address, home address and IP address. The first data set is referred to as the Identity Graph. It validates digital identity elements and how they are linked to one another by using third-party identity data sourced from authoritative data providers. These global providers have been vetted with rigid acceptance criteria to ensure accuracy and security compliance.

However, this is not enough. In the digital world, this only reveals half the picture. These core elements are just the starting point given that fraudsters could still obtain these data points and pretend to be someone they are not.

That's why Mastercard Identity's second unique data set, the Identity Network, looks at how the identity elements are being used online, whether by a legitimate customer or by a fraudster. It leverages a network made up of hundreds of millions of monthly customer queries to derive activity patterns and understand how the identity elements are being used in the digital world. A fraudster may be able to use data from a legitimate customer, but their behaviors do not match that person's behavior patterns. This is why they get caught.

Validate digital identities with a multi-layered approach

Preventing fraudsters from taking advantage of your digital platform requires a multi-layered approach to identity validation. This means designing an identity verification solution that is all encompassing, with a combination of rules-based decisioning and machine learning for comprehensive fraud prevention. A multi-layered approach is usually outfitted with a combination of internal and third-party identity data. At a minimum, rules are put in place to weed out known bad actors, such as those that have been blacklisted.

However, synthetic identities typically do not exhibit characteristics that would place them onto a blacklist. In these cases, a more sophisticated measure that leverages machine learning using dynamic identity attributes could add the necessary layer of security; helping delineate the good from the bad and identify potential fraudsters. Platforms that take a strategic proactive approach in fighting fraud could go a long way in battling this unique set of fraudsters.

Conclusion

Fraudsters that do not look like fraudsters are a challenge for companies around the world. Not only do these synthetic identities look real in many respects, but they also contain attributes of legitimate customers. To fight against this ever-growing species of cybercriminal, companies need to recognize the limitations of strictly evaluating static identity attributes.

By looking at each customer or transaction with a multi-dimensional lens that draws on dynamic identity attributes and their relationships to each other, businesses set themselves up to be better equipped to combat synthetic identity fraud. Additionally, companies must also look at their fraud-prevention solutions holistically to ensure there are not any gaps that fraudsters could exploit. Remember, it’s a game of chess.

What is your next move?

About Mastercard Identity

Today's digital economy opens a world of opportunity for everyone everywhere to connect. Mastercard Identity securely and seamlessly connects people with merchants, banks and businesses worldwide — enabling them to interact with confidence how, where and when they want. Powered by global identity technologies, data and insights, machine learning scores and biometrics, organizations worldwide can verify and authenticate more genuine consumers and prevent fraud in real-time. From the initial account opening through account changes – and across the entire payment transaction and fraud ecosystems, Mastercard Identity instills trust on both sides of the interaction.