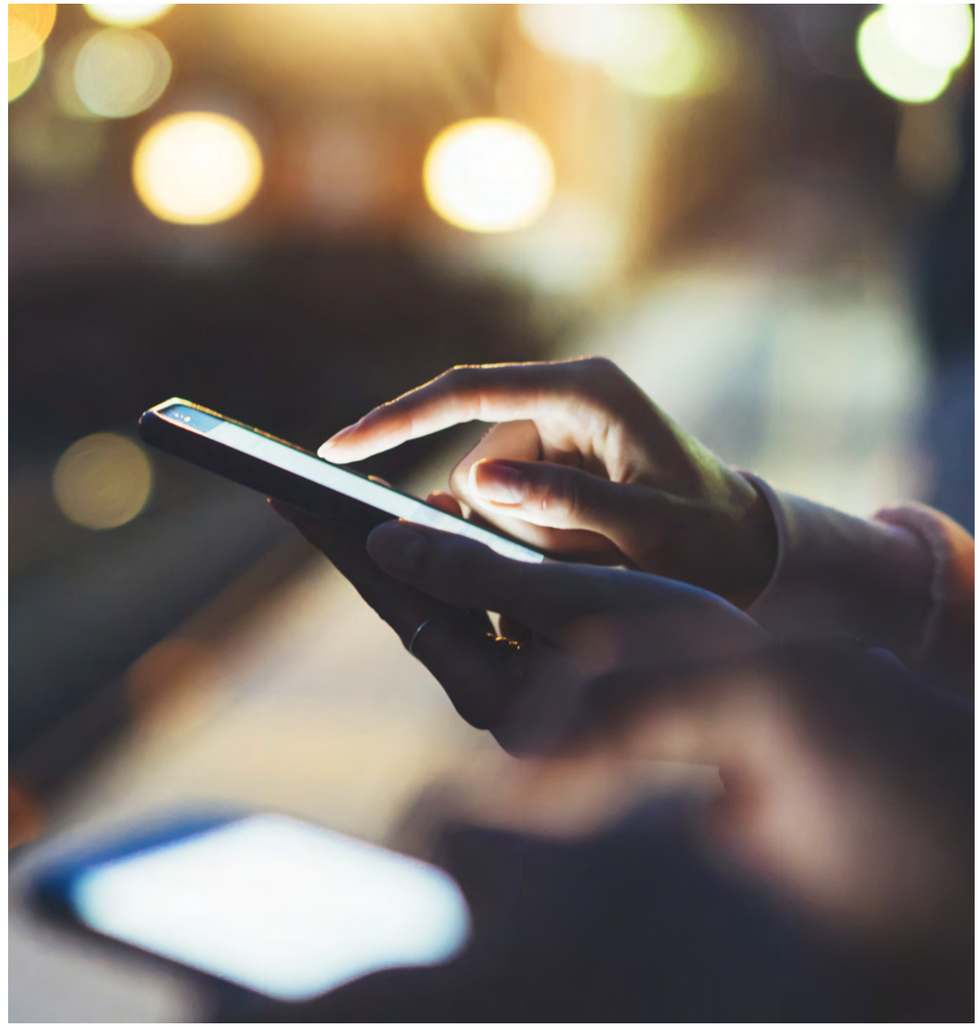
Synthetic Identity Theft

Upgrading Your Identity Verification Toolbox to Combat This Growing Threat

Learn how this fast-growing crime threatens every business

There is no question that synthetic identity theft — crime perpetrated by bad actors who use real and fake personal information to craft an authentic-looking digital identity — is a fast-growing crime. The 2017 Equifax breach alone exposed the Social Security numbers of more than 140 million Americans, and those affected are still battling claims three years later.

Data breaches are not unique to the US — companies around the world face similar challenges. Personal information exposed from data breaches often winds up for sale on dark web marketplaces, which is where fraudsters can buy the data they need to commit synthetic identity theft.

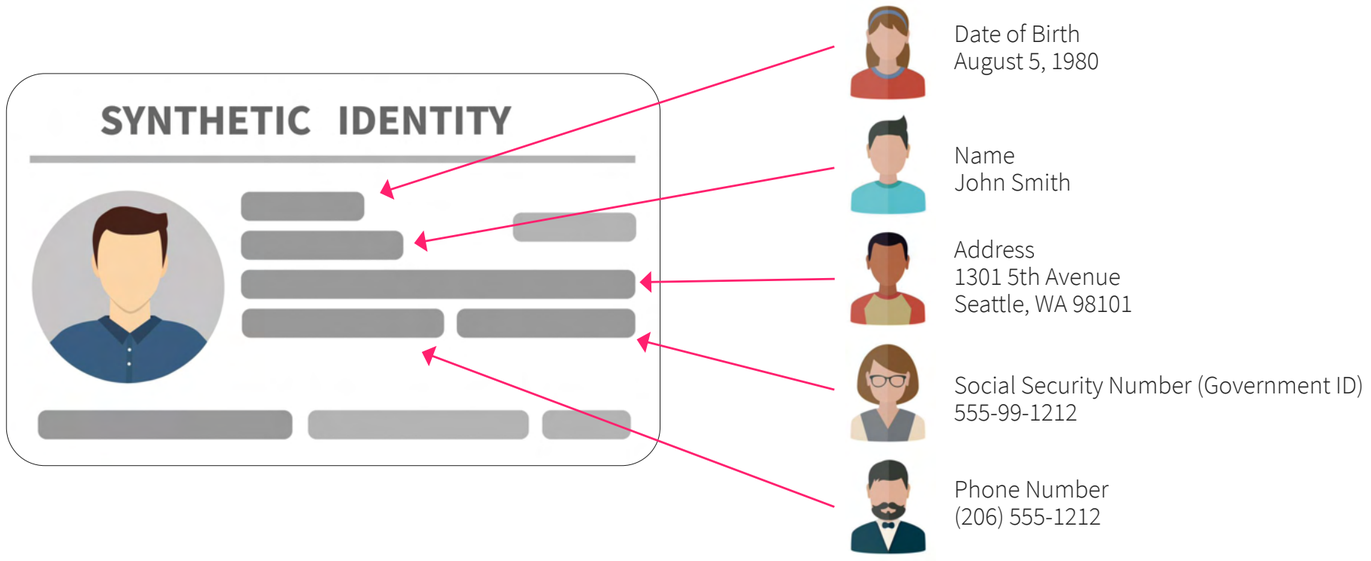


Source: BBC, “Equifax finds more victims of 2017 breach” https://www.bbc.com/news/technology-43241939 2

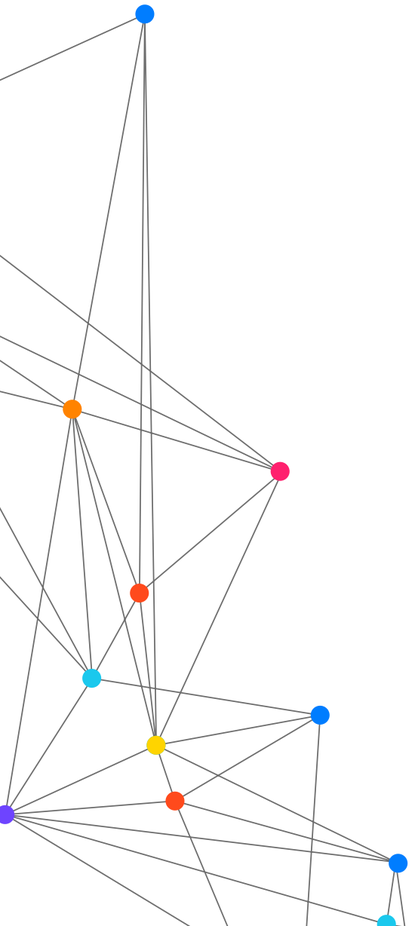
What is synthetic identity theft?

Synthetic identity theft occurs when a bad actor uses a composite of personal information from real people to create an authentic-looking identity. The fraudster may also use fake personal information to round out the identity. Personal information that a bad actor uses may include name, national identification number (NIN), birth date, and home address. For example, In the US, a scammer 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 newidentity. Similarly, in the UK, a bad actor might use a stolen NIN from one person and a home address from another to form afictitious profile. When the attributes are combined, the identities may appear legitimate given that parts of the whole are real.

SYNTHETIC IDENTITY – A "REAL" IMPOSTER



Synthetic identity theft is difficult to fight



1. FRAUDSTER SOPHISTICATION

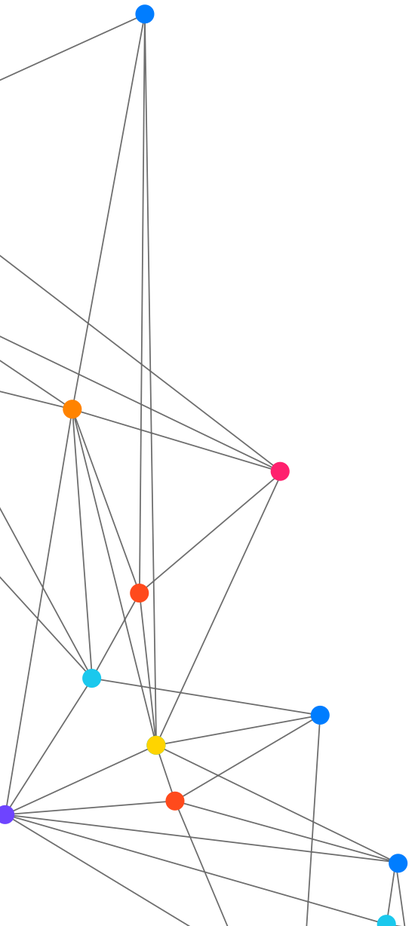
First and foremost, fraudsters are sophisticated and patient enough to carry out long-term, large-scale fraud. They will take months or years to nurture an identity to preserve the integrity of its profiles and establish credibility. They've gotten so good at this type of fraud that in the U.S., synthetic fraud alone now accounts for 10%–15% of charge-offs in a typical unsecured lending portfolio.

Second, synthetic identities consist primarily of real personal information and often include a stolen government-issued identification number. IMaking detection more difficult is that some countries currently do not have an easy way to validate these unique identification numbers.

2. UNDETECTABLE FRAUD

In the U.S., fraudsters often steal the Social Security numbers of children. Most children do not have a credit history, so scammers use their identifier as a means for 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 loans.

Typically, when a person's identity is compromised, the first sign of realizing such behavior would be a notification from that person via a complaint or a concern. However, if the person whose identity has been synthetized is a child without their own financial accounts, then there's no way for them to notice fraudulent activity and flag it.



3. DECEPTIVE BEHAVIOR

Fraudsters operate as a wolf in sheep's clothing. When their identities are questioned, they continue to pretend to be the good customer they claim to be. If they're able to convince the merchant their transaction was falsely declined, the interaction becomes a way to further build trust and credibility. Many fraudsters also take extra care to maintain strong credit scores for their synthetic identities.

For example, in the US, a scammer might spend years building a high FICO score. In Germany, a scammer 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, it is not so much for fraudsters who are well-versed in the field. Fraudsters often use automated tools such as bots to quickly create hundreds, sometimes thousands, of online accounts or to submit online applications. They also use device emulators to reset device IDs and mimic behaviors of good consumers to evade detection.

4. TRADITIONAL METHODS NO LONGER WORK

Fraudulent behavior is not new — but synthetic fraud is. Traditional fraud tools that were designed to capture stolen identity activities do not serve well in solving synthetic identity problems. With stolen identity information, fraudsters act quickly to impersonate the owner and capitalize on the opportunity. On the other hand, synthetic identity fraudsters 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 transacted into data attributes, as shown to the right.

Data inconsistencies — such as identity elements not matching with reality — are strong signals for both stolen and synthetic identities. Their value is the highest when used to detect synthetic identities, however, given the fabrication of those identities. A relative increase in usage velocity of an identity for fraud is a strong signal in the case of stolen identities, since fraudsters try 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.

Source: AnnaMaria Andriotis and Peter Rudegeair, "The new ID theft: Millions of credit applicants who don't exist," Wall Street Journal, March 6, 2018, wsj.com.

How do fraudsters use synthetic identities?

Banking and lending

Fraudsters often use synthetic identities for 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 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, the fraudsters bust out, maxing out all the credit lines at once or within a short time frame.

To the lenders, the accounts have 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 an estimated $6 billion every year.

One of the largest fraud schemes involving synthetic identities led to confirmed losses for businesses and financial institutions totaling more than $200 million. The scammers fabricated more than 7,000 false identities, which were used to obtain thousands of credit cards.

"One of the common uses of synthetic identities is to commit account opening fraud. It is how fraudsters gain access to a slew of exploitable opportunities.

From establishing a bank account to preparing for loan applications or money laundering to creating online accounts for fraudulent transactions, fraudsters are creative in how they make use of the system."

*Source: CNBC, "Criminals are using 'Frankenstein identities' to steal from banks and credit unions,"https://www.cnbc.com/2020/01/16/criminals-using-frankenstein-identities-tosteal-from-banks.html

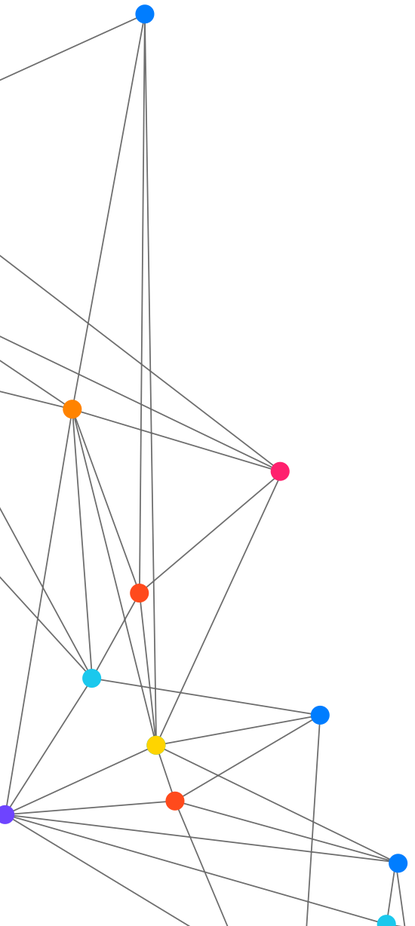
**Source: US Department of Justice, "Leader Of International, $200 Million Credit Card Fraud Scam Sentenced To 80 Months In Prison," justice.gov/usao-nj/pr/leader-international200-million-credit-card-fraud-scam-sentenced-80-months-prison7

Online marketplaces and ecommerce

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, the fraudster buys 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, and the suppliers to the fraudulent merchants are hit with chargebacks because of the invalid credit cards.



Credit repair services

Fraudsters sometimes scam consumers through credit repair companies. They charge a fee to fix a consumer's bad credit, but 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 synthetic identity farms in disguise and harm the consumers who use them.

Battling synthetic identity theft

Fraudsters are often ahead of the game when it comes to anticipating the obstacles they will face with modern-day fraud detections. So, how can you address this issue? What are the gaps? How can you be in front of the problem before it occurs?

It is like a game of chess: they think three steps ahead so you need to think four steps ahead to trump 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 means getting their hands on that information is relatively easy.

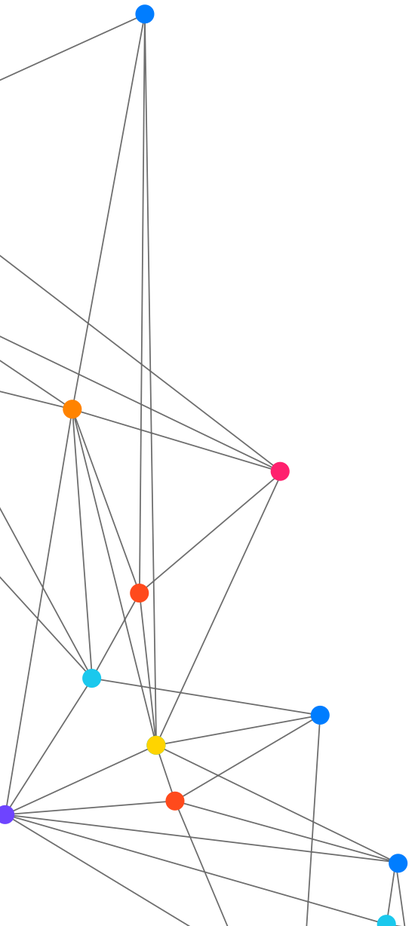
A static identification attribute that does not change over time is useful for synthetic fraud because once the fraudsters have it, they can use it until they're caught without fear of it changing. On a smaller scale, if you got hold of a friend's Social Security number and celebrated his birthday last week, you could technically pretend to be your friend in many instances.

Some companies leverage these static identity attributes to verify identities and that is, in part, the shortfall. These identifiers alone are vulnerable to fraud because of 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.

At Ekata, 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 trace of your DNA behind 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 that we consider to be 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 detect and combat synthetic identities



Synthetic identities behave differently than other types of stolen identities, which generates different types of risk signals. Importantly, the relationship between a synthetic identity's name and email or name and phone may only exist once as those attributes are cycled through to be used in other identities. This is why the use and observations of dynamic identity attributes can help detect synthetic identities.

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.

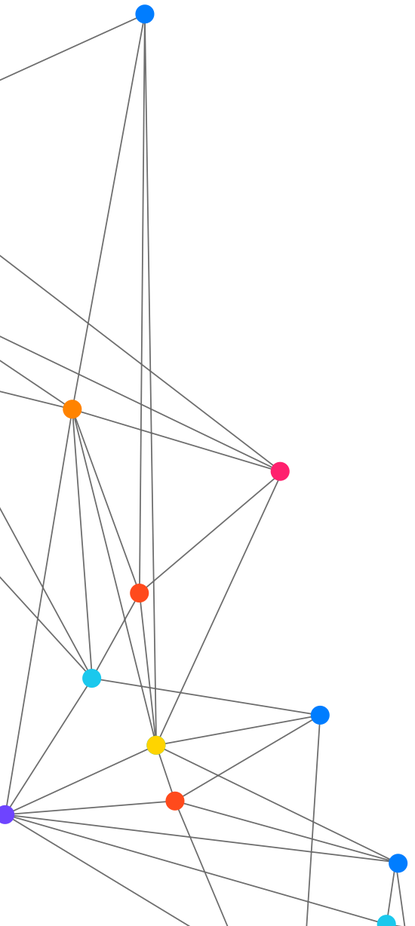
Based on what the customer has entered in a record — whether it be an account opening application or a transaction — the information (name, email, phone number, and address) can be evaluated. The results rely on probabilistic risk assessment and can provide predictive signals of potential fraud by validating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

How does it work?

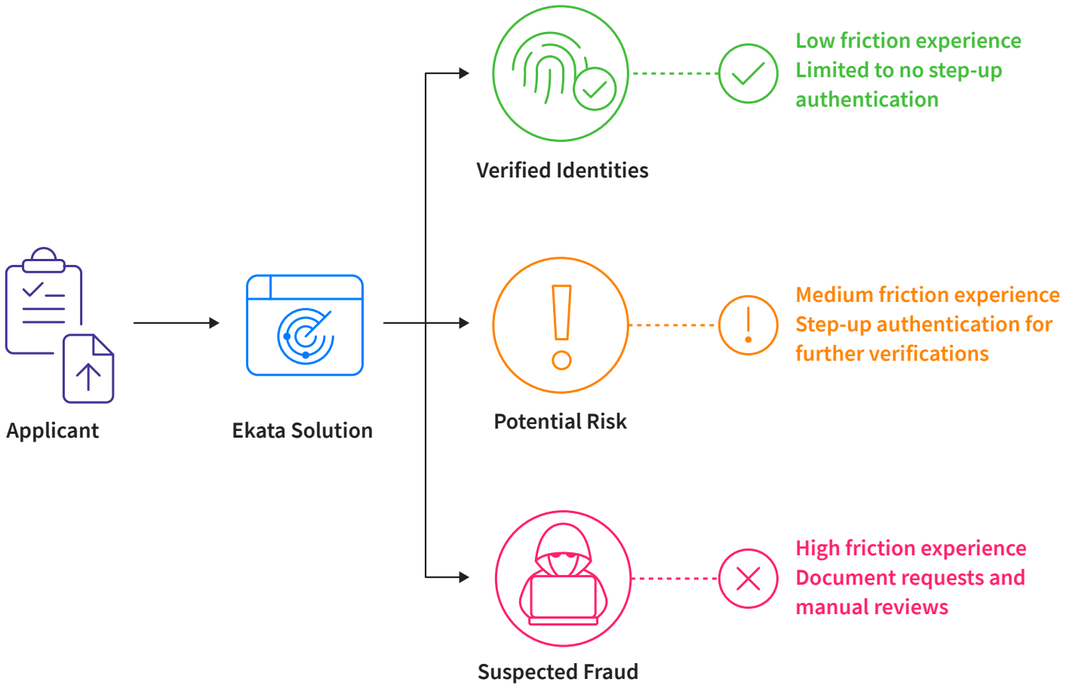
Ekata has built two differentiated data sets around five core elements: name, phone number, email address, home address, and IP address. The first data set is referred to as the Identity Graph. It validates digital identity elements and how they are linked to one another by using third-party identity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

But in the digital world, this only shows 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 Ekata's second unique data set, 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 over 400M+ monthly customer queries to derive activity patterns and understand how the identity elements are actually being used in the digital world. A fraudster may be able to use data from a legitimate customer, but they do not act like that person. This is how they get caught.



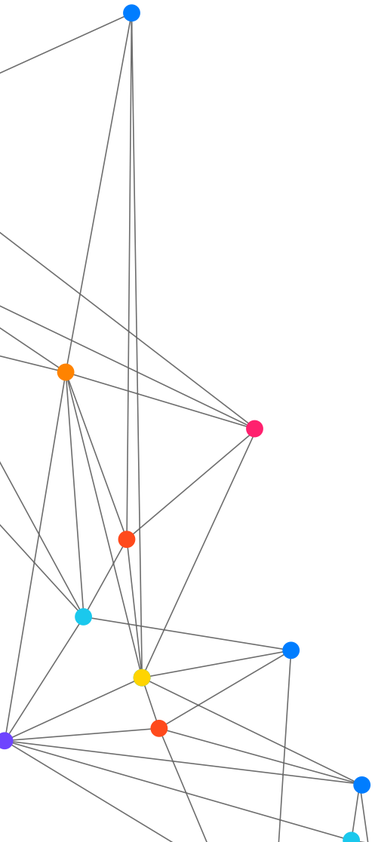
DETERMINING RISK DURING ACCOUNT OPENING



Validate identity 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-validation solution that is all encompassing with a combination of rules-based decisioning and machine learning for your fraud-prevention efforts. A multi-layered approach is usually outfitted with a combination of internal and third-party identity data. At the minimum, rules are put in place to weed out known frauds, such as those that have been blacklisted.

Synthetic identities typically do not exhibit characteristics that would place them onto a blacklist, however. In these cases, a more sophisticated measure that involves machine learning using dynamic identity attributes e could add a layer of security to help delineate the good from the bad and identify potential fraudsters. Platforms that take a proactive and mindful 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 emerging and ever-growing set of fraudsters, companies need to recognize the drawbacks and 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 prepared for synthetic identity fraud. But that is not all. Companies must also look at their fraud-prevention solutions holistically to ensure there are not any gaps that fraudsters could exploit. Remember, it is like a game of chess.

What is your next move?

About Ekata

Ekata Inc., a Mastercard company, is a global leader in digital identity verification solutions that provide businesses worldwide the ability to link any digital interaction to the human behind it. The Ekata product suite is powered by the Ekata Identity Engine, comprised of two data assets: the Ekata Identity Graph, a proprietary data store of over 7 billion entities that validates digital identity elements and their interlinkages; and the Ekata Identity Network, a collection of over 16 billion identity elements and machine learning models that surface patterns of their use online. Ekata's award-winning global product suite includes high-scale and low-latency APIs used in transaction, monitoring, and customer onboarding, along with its Pro Insight SaaS solution for manual fraud review. These solutions empower over 2,000 businesses and partners, like Alipay, Equifax, and Microsoft, to combat cyberfraud and enable an inclusive, frictionless experiencefor their customers in over 230 countries and territories.

Contact us to learn more.
www.ekata.com | 1.888.308.2549