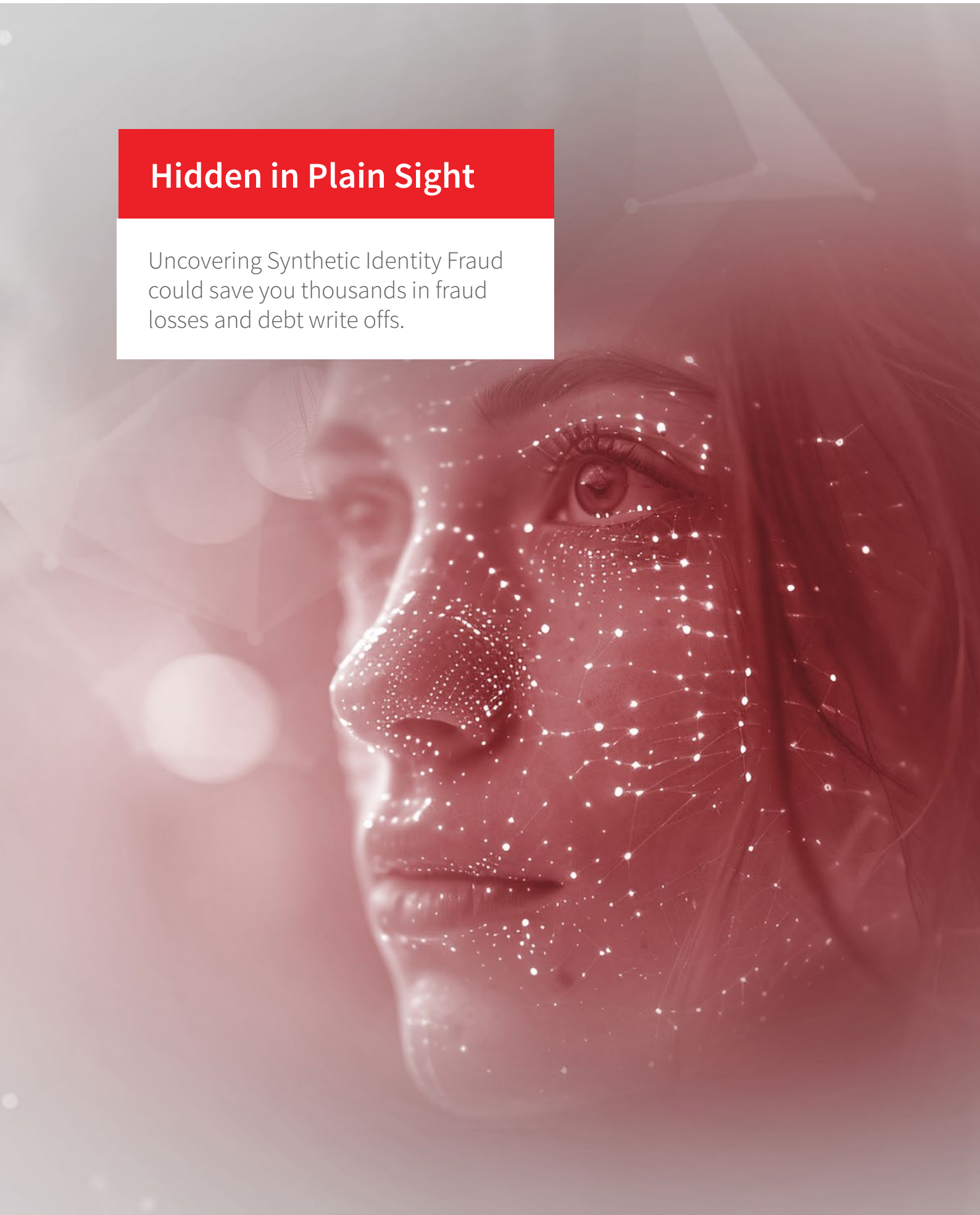
LexisNexis®
RISK SOLUTIONS

Hidden in Plain Sight

Uncovering Synthetic Identity Fraud could save you thousands in fraud losses and debt write offs.



Contents

1. What is synthetic identity fraud? 2

- A perfect crime? Low risk, high reward for fraudsters
- Frankenstein identities: manipulated or manufactured
- The tell-tale signs: high-risk indicators

2. Are you letting synthetics slip through the net? 7

- 3 million highly suspicious identities
- Fastest growing type of fraud
- Industrial-scale manufacturing and maturing of synthetic identities

3. What does this mean for your organisation? 10

- The dangers of synthetic identity fraud
- Up to 15% of your debt write-offs[1] could be synthetics
- Balancing approval speeds with increased confidence

4. How much of a problem is synthetic identity fraud for your organisation? 12

- Free initial assessment to help you quantify the problem
- Predictive analytics to identify risk factors and flag suspicious accounts
- A fraud model, tailored to your needs

[1]Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise: Julie Conroy, Aite Group, 2021

1. What is synthetic identity fraud?

The perfect crime? Low risk, high reward

Imagine a fraud that takes some time to set up, but that can be carried out at high volume and where the returns are substantial – far bigger than with most identity thefts but with only a fraction of the risk.

Unlike common identity or credit card theft, the criminals aren't up against a short deadline to make as much money as they can before the true identity or card holder finds out and reports the issue. With this type of fraud, the fraudsters invest effort and money upfront but when they finally bust out, the rewards are big, and they can simply vanish into thin air.

By applying for credit and accounts and making payments on time, they establish strong credit profiles, building up the trust of lenders and other institutions. On the face of it, they're not doing anything suspicious. In fact, just the opposite. They look and act like the perfect customer.

The fraudsters are in it for the longer term – months, if not years, but the promise of high returns makes it all worthwhile. And by industrialising their approach, they can make sure they have a full production line with new identities being built and nurtured as others cash out.

Slipping under the radar

Even the increasingly sophisticated fraud prevention controls operated by banks and other financial institutions are unlikely to detect them once they're 'through the door'. Financial institutions might be looking at behaviours and ability to pay, but how do you assess 'intention to pay'?

So, when they're ready to cash out, the fraudsters make a big hit - maybe a significant credit purchase, or a large loan. Nothing about this seems unusual to the lender. That is, until the customer unexpectedly default on their payment, at which point they're gone. Vanished.

When the lender pursues the debt, they can't trace the customer, as they never really existed. Worse still, the institution may not realise even then that the debtor never existed and might just write the debt off as a credit default, not even a fraud loss, believing their good customer fell on bad times.

No-one suspects a thing.

The likelihood is that the Credit and Fraud departments of large financial institutions don't work very closely together on a day-to-day basis, or share data, so they quite possibly won't even consider this a fraud problem. They'll see increasing volumes of charge-offs, but with no obvious impact on fraud losses.

So, the business is unaware it has a fraud problem. Customers aren't complaining. Departments with limited budget aren't looking to spend on a problem they don't know they have. Meanwhile credit losses spiral, impacting the bottom line as Collections departments struggle to chase up their bad debts.

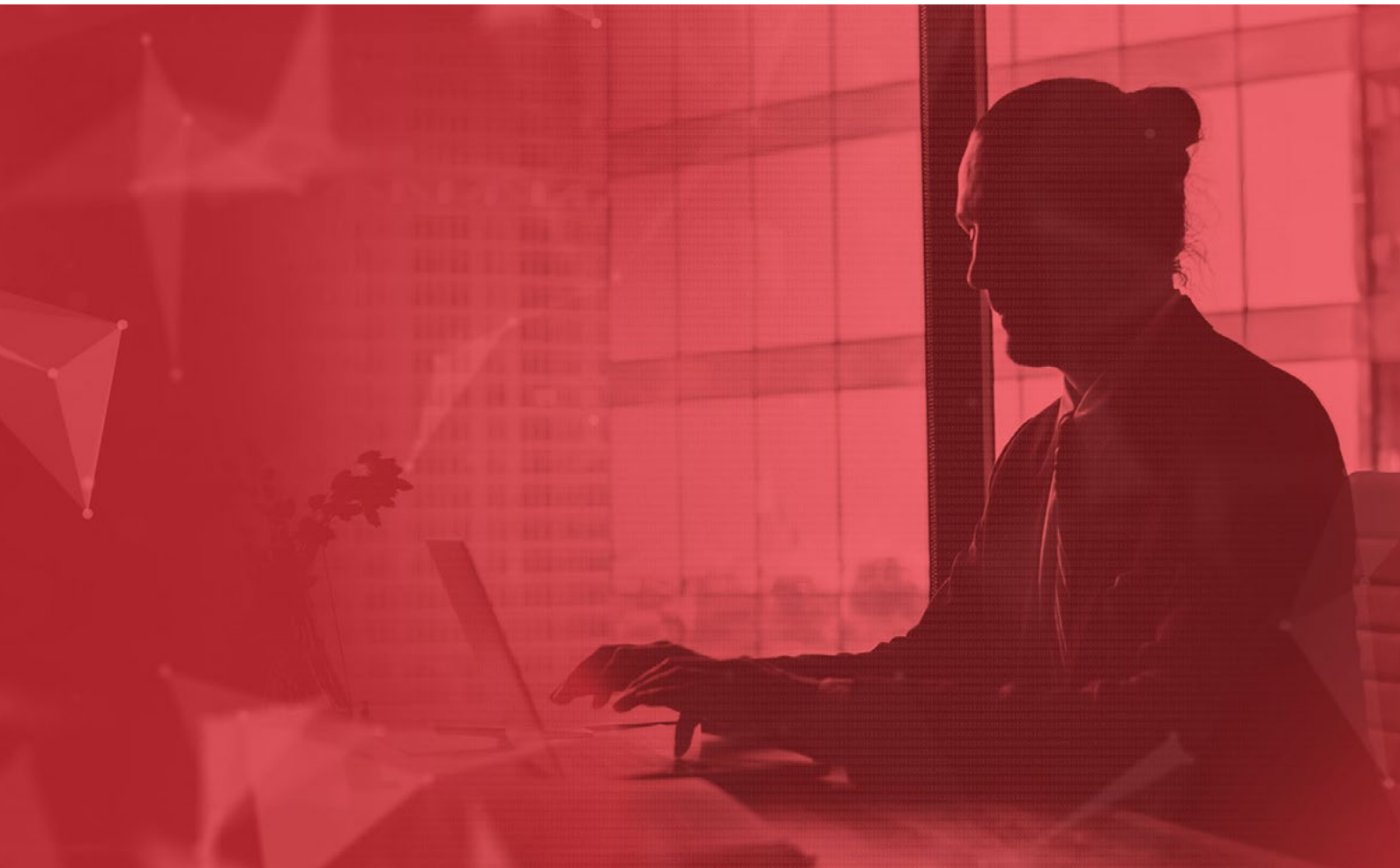
‘Frankenstein’ identities

Often referred to as ‘Frankenstein’ identities, synthetics are fictitious identities that don’t relate (at least not directly) to any real living person. They contain elements of truth, designed to spoof credit checks and build enough legitimacy to present as trustworthy during identity checks carried out at onboarding.

Synthetic identities are typically created using **manipulated** or **manufactured** details, each posing slightly different challenges for businesses.

- **Manipulated synthetic identities:** Individuals often use manipulated identities to hide a previous history and gain access to credit and they may or may not be used with malicious intent. Individuals with bad credit histories may create fictitious identities to be approved for new credit for legitimate purchases that they intend to repay. The good news for enterprises is that manipulated identities can be detected. The key to identifying manipulated synthetics is that they often collide with the real identity they are augmenting and do not pass validity checks.

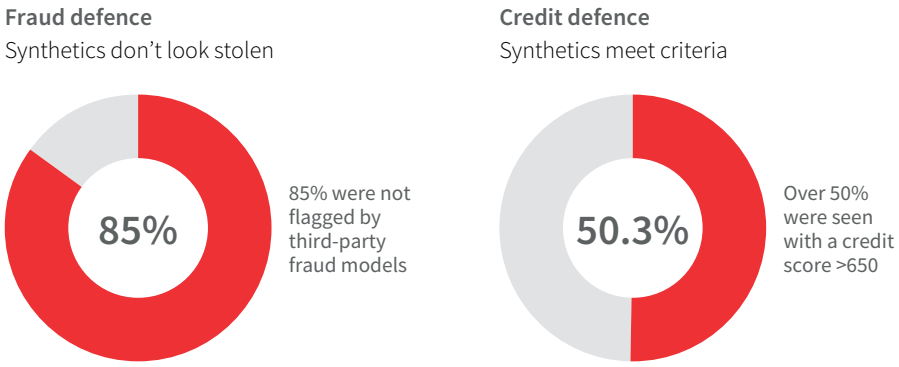
- **Manufactured synthetic identities:** Identities created by combining real identity data with synthetic components, or completely made up with fake information. This category represents a more pronounced and damaging business risk. Manufactured synthetic identities are often generated and actively managed by organised fraud networks. Fraudsters expertly combine fictitious and real identity elements to create a new identity that is not associated with a real person and difficult to detect with static fraud solutions.



Manipulated synthetic identities can be detected by more robust fraud and identity checks, as they often collide with the true identity they are imitating. The challenge with manipulated synthetic identities is that they are not accurately assessed according to their true credit risk level, which might lead them borrowing beyond their means and an inability to repay.

Manufactured synthetic identities, made up of a broader mix of stolen, or completely fabricated information can be much harder for fraud checks to spot. In fact, according to a study carried out by LexisNexis Risk Solutions in the US[2], 85 per cent of synthetic identities were not flagged up by third-party models.

Traditional approaches overlook synthetic identity fraud



Source: LexisNexis® Risk Solutions, Internal Research, March 2021

Legitimising the synthetic identity and building a credit profile

Once created, fraudsters look for ways to build the credit score for the synthetic identity, perhaps through 'approval shopping' where they manage to establish credit with a lender who will approve 'credit invisibles' that other credit bureaus cannot score. Another tactic employed by the fraudsters is 'credit piggybacking', where they add the synthetic identity as an authorised user to a legitimate account.

Once the synthetic identity is 'live', the fraudsters will systematically apply for lines of credit to build the credit score, incrementally increasing the value of credit, before maximising gains and cashing out.

[2] LexisNexis® Risk Solutions, Internal Research, March 2021

The tell-tale signs: high risk indicators of synthetic identity fraud

Masking a synthetic identity as an emerging consumer makes it easier to elude detection. The threat is further complicated because losses tied to synthetic identities are often treated as credit losses since synthetic identities are not associated with real consumers who report a stolen identity.

Nevertheless, there are a number of defining characteristics that help distinguish legitimate thin-file applicants from synthetic identities:

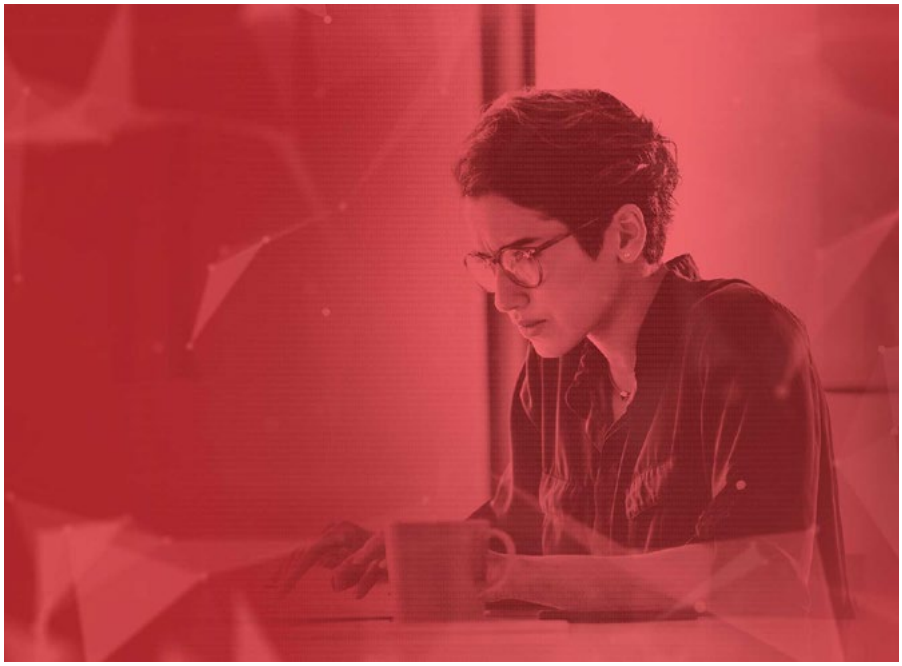
- **Lack a 'life story':** The network emergence path of synthetic identities is different from legitimate identities and their behaviour is atypical. For instance, they may suddenly appear in the ecosystem later in life and their identity profile does not follow the logical path that might be expected through the stages of a regular person's lifecycle.

- **Proof of existence:** They tend to have no government or trusted 'proof of life' record for the identity, not being on the electoral roll or holding a passport or driving licence, with the predominant proof of existence being CRA records.

- **No family connections or associates:** Synthetics often have no evidence of family – parents siblings, partners or associates.

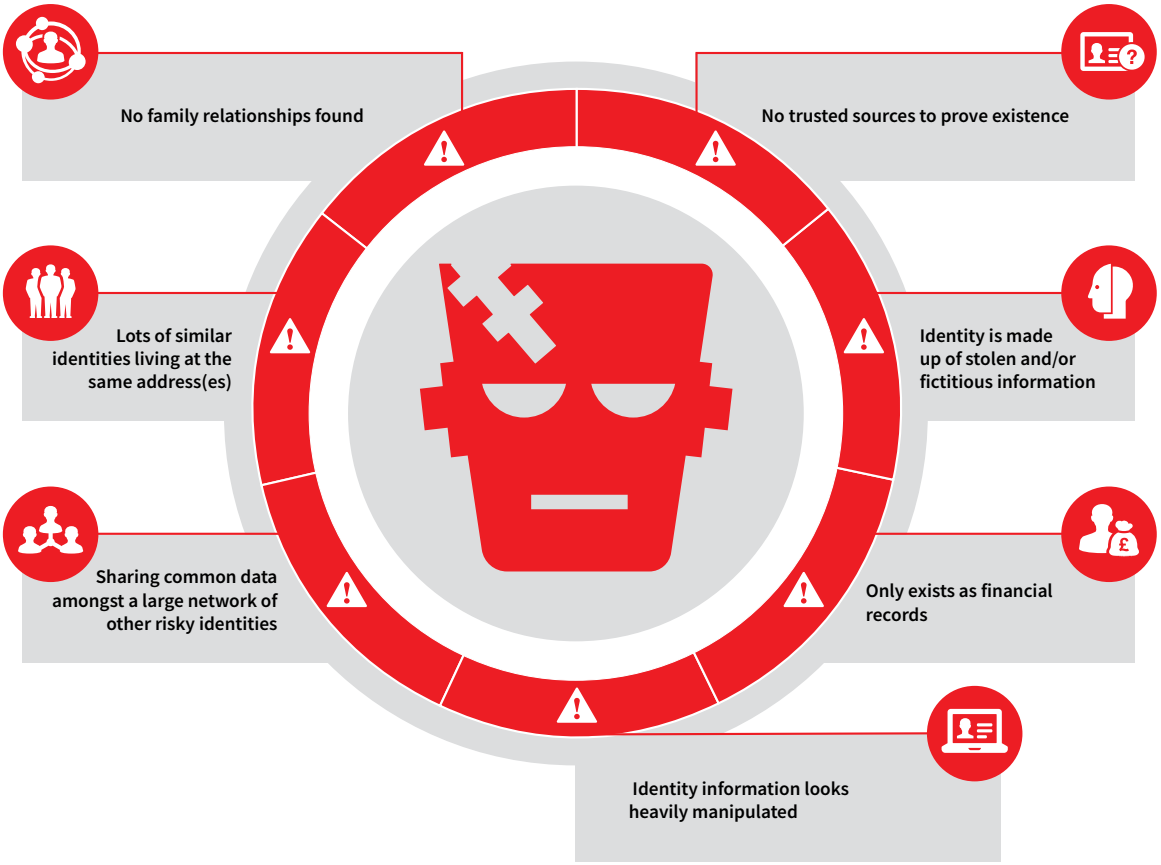
- **Manipulated details:** Personal identifiable information (PII) shows signs of manipulation – e.g. lots of variations in spelling of the same name, address and contact details.

Scanning for these sorts of high-risk factors can help to build compelling evidence of suspicious activity that strongly indicates synthetic identities are present.



DNA of a Synthetic Identity

Seven telltale signs for spotting Frankenstein identities



The types of scenarios we might find in relation to synthetic identities are as follows:

Let's assume we have 3 sets of dominant PII

- Sherlock Holmes, 01/04/1965, 122b Baker Street, Sholmes@detectiveagency.co.uk, 0771234567
- Jim Moriarty , 05/08/1953, 125 Regent Street, jMoriarty@nemesis.co.uk, 0798765432
- John Watson, 12/12/1973, 24, York Street, JHwatson@sidekick.co.uk, 0787654321

We might then see combinations of those identities, for example:

- Jim Watson, 12/12/1993, 125 Regent Street, jMoriarty@nemesis.co.uk, 0798765432

We may also see a mixture of real and fictitious details, such as the following:

- Sherlock Watson, 12/12/1993, 07 York Street, madeupemail@mue.com, 0792837465

In this way, a network of synthetic identities is created using the same 3 dominant identities, which are co-mingled, recycled and manipulated as fraudsters try different combinations to try to gain access to credit.

Digital applications for credit products create a data footprint. Fraudsters will make repeated applications to build a data profile for a fake identity until a credit product can be secured.

(n.b. These details relate to fictitious characters and are intended only for demonstration purposes.)

2. Are you letting synthetics slip through the net?

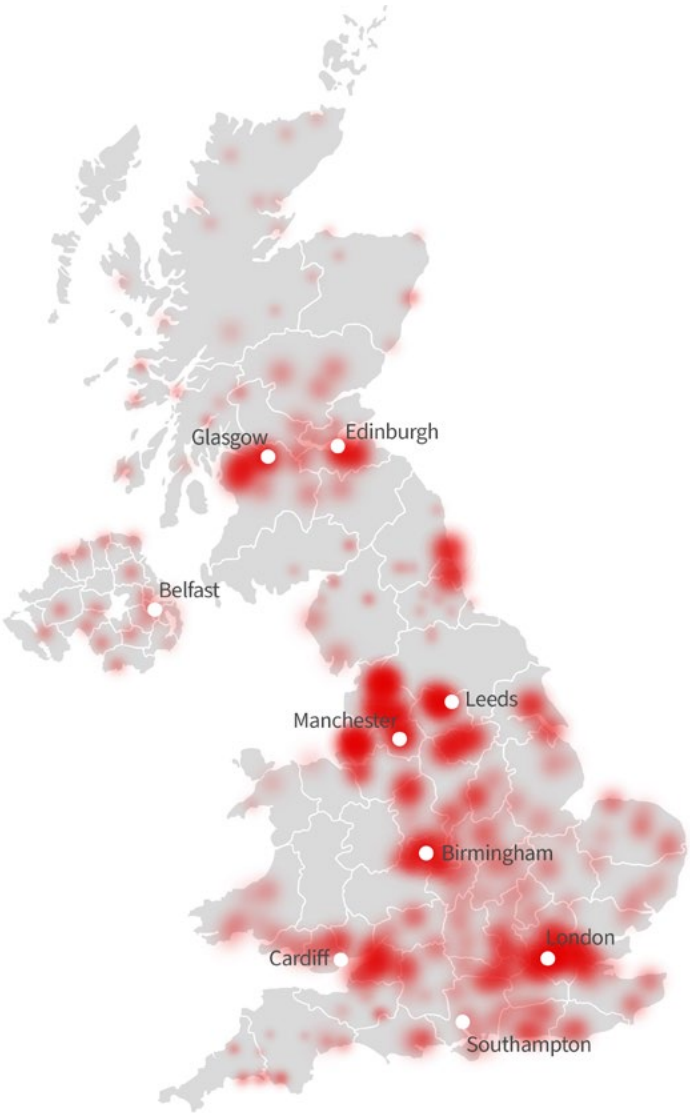
3 million highly suspicious identities

Synthetic identity risk is more prevalent across the UK than previously thought and is likely to continue to grow.

Our analysis of 72 million consumer profiles has revealed almost 3 million identities in circulation in the UK displaying several high-risk factors that point strongly at the presence of synthetic identity fraud.

Synthetic identities are not just seen in highly populated areas but are evident throughout the UK.

Geographic spread and saturation of highly likely synthetic identities



Fastest growing type of fraud

Synthetic identity fraud is widely thought to be one of the fastest growing types of fraud, with the rise in synthetic identities being regarded as one of the top three challenges to identity verification[3] by European financial services institutions.

LexisNexis® Risk Solutions data shows a major rise in synthetic identities in the UK in the past 3 years. Our analysis reveals that the proportion of 'highly probable' synthetic identities, displaying seven high-risk indicators, increased nine-fold (527%) between 2020 and 2023. Over the same period, the number of 'highly likely' synthetic identities, displaying five or six high risk indicators increased six-fold. Identities displaying three or four high risk indicators – still very likely to indicate a synthetic identity – quadrupled to over 2.5 million within the same timeframe.

Industrial-scale manufacturing and maturing of synthetic identities

We're also uncovering increasing evidence that fraudsters are scaling up their operations and industrialising the production and nurturing of synthetic identities, through synthetic factories.

Using readily available personally identifiable information (PII) as their raw material, the manufacture of new synthetic identities is big business for fraudsters. Data breaches make it easier to commit synthetic identity fraud. According to Statista, 67.7 million UK data records were exposed from 2020 to 2023.

Our analysis revealed multiple examples of properties, often in isolated rural locations across the UK, with multiple identities linked to them, highly suspected of being used as 'synthetic farms' to develop and mature the credit footprints of synthetic identities.

One farm in Chichester displayed 439 unique entities transacting at the property over seven years. These identities were constructed on thin financial data, such as credit bureau and short-term loan data: 85% credit bureau, 5% short term loans, 5% government sources, 5% other. They had no other 'proof of life' from electoral roll or government sources.

Up to 2016, we saw a consistent Electoral Roll footprint for a family living at the farm, followed by a major increase in the number of identities and records. Notably, 8% of these identities are also seen within another location, just outside Dundee, with a similar make up. Our analysis identified a number of these apparent linkages between synthetic farms operating across different parts of the UK, suggesting broader organised criminal networks operating across multiple geographic locations.

A common characteristic of synthetic farms is often an easily accessible and unsecure post box, allowing fraudsters to intercept mail.

[3] LexisNexis Risk Solutions EMEA True Cost of Fraud report

Aside from synthetic farms, the analysis also revealed widespread evidence of suspicious ‘synthetic houses’ – residential properties with over 50 identities ‘residing’, typically clustered within a small geographic area.

One example of a large synthetic ring in Oxford comprises a network of nine terraced style properties within the same postcode. In 2018, three dominant sets of manipulated personally identifiable information within one of the properties started to create over 150 unique entities, with over 450 credit footprint records. Only two of the identities contained any trusted sources. High levels of name and date of birth manipulation were evident, with other credit application fields such as reason for loans, income brackets and job type, cycling through a limited number of common responses.

Another example we uncovered was in relation to a typical 3-bedroom house in London, with 1653 unique identities linked to the address over the past 20 years. Only 10 of these identities could be validated through trusted government sources. Over half of the identities have only one associated record. Outside of the core 10 validated identities, the sources are entirely made up from credit bureau and/or short-term loan records. This address appears to be used repeatedly to gain access to credit, though credit providers would not necessarily see this trend.

3. What does this mean for your organisation?

The dangers of synthetic identity fraud

In a saturated market, where competition is rife, organisations rely on their ability to attract new customers to meet growth goals. However, the highly coveted new entrant demographic creates the perfect cover for enterprising fraudsters to perpetrate lucrative synthetic identity fraud schemes.

The true danger of synthetic fraud is that, unlike third-party fraud where an entire identity is stolen and used to defraud enterprises and victims, synthetic fraud frequently has no specific consumer victim. That can sound like a good thing – until you realise that consumer victims are a critical tool in detecting and stopping fraud. The lack of a clear victim presents two challenges to enterprises.

- Without a consumer to alert an organisation of fraudulent activity during account life, fraudsters can use synthetic identities to keep accounts open for months or years, garnering credit line increases and improved credit standing, only to eventually max out the credit line and disappear without a trace.

- Once the account charges off, synthetic frauds are often categorised as bad debts – since there is no clear evidence of fraudulent activity. For enterprises, this makes it difficult to identify a synthetic fraud problem – and even harder to know if new defences are proving effective.

These examples show the difficulty in tracking and quantifying losses from synthetic identities. Additionally, there are often inconsistencies within organisations on what constitutes a synthetic identity, and even disagreement as to whether this is a fraud or credit problem. Without a paper trail leading to a real person, the true victims of synthetic identity fraud are the lenders and service providers who are left to absorb what can be high-frequency and high-value losses.

3 million UK consumers may be synthetic

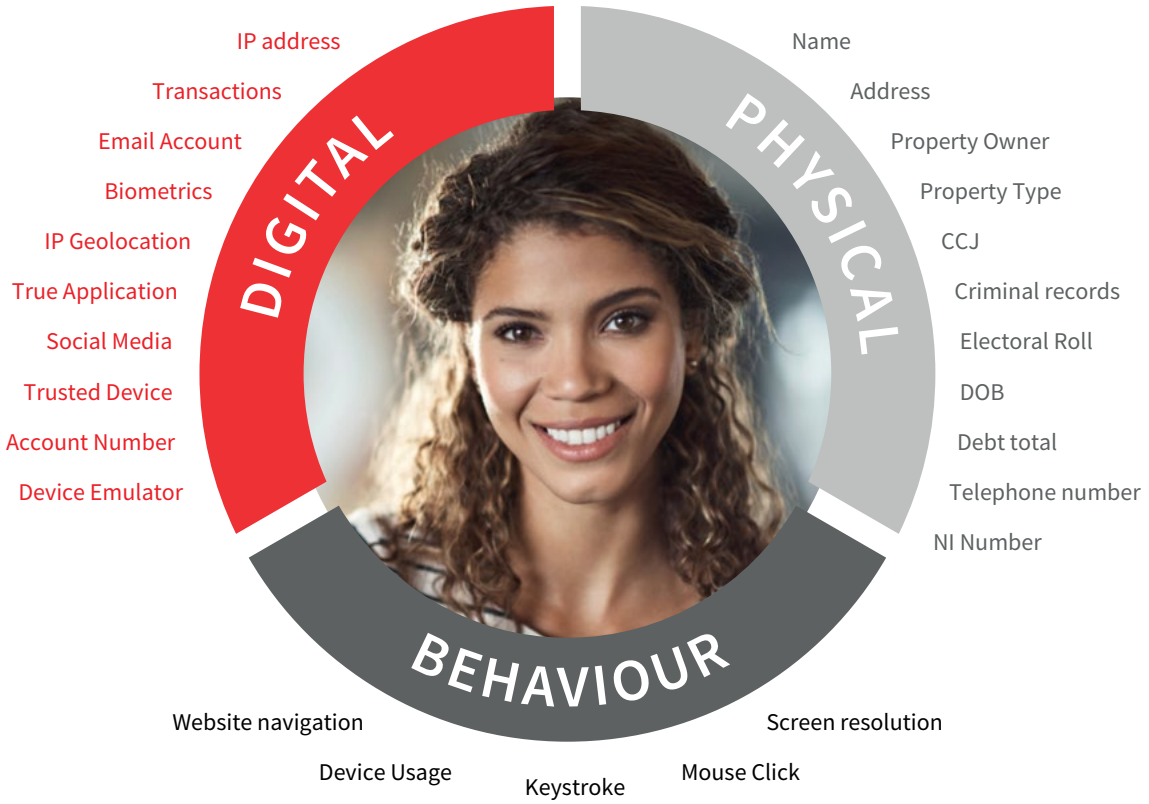
What all of this means for your organisation is that you could well be harbouring synthetic identities within your customer base. They will appear and act like good customers, but could be preparing to cash out at any moment, leaving you with irrecoverable debts. According to a 2021 report by analyst firm, Datos (formerly Aite), around 15% of all debt write-offs could be synthetic fraud. The report went on to predict that in the U.S. synthetic fraud for unsecured U.S. credit products will grow to US$2.42 billion by 2023.

Balancing approval speeds with increased confidence

Competing more effectively in the emerging consumer market starts with an accelerated customer acquisition process that accurately recognises legitimate customers, speeds up approvals and mitigates fraud threats. You need a fraud prevention approach that will assess applicant identity and application behaviour at onboarding, as the application occurs, allowing you to expedite legitimate applicants without creating unnecessary friction or delay in the process.

Breadth and depth of data is key to highlighting synthetic identity risk. Networks that systematically pool application data and fraud feedback, and resolve consumer identity more accurately, help to avoid synthetic identity fraud risk while accelerating approvals and onboarding. The bigger and fresher the networks, the more reliable the risk signals.

The key to determining identity risk is referencing multiple 'proof points'



Differentiated insights into critical data interconnections, inconsistencies and fraud patterns in applications allow fraud teams to focus on high-risk applications more efficiently, while legitimate applications proceed with less friction and delay.

This is where LexisNexis Risk Solutions can help.

Let's start by helping you assess how much of a problem synthetic identity fraud is for your organisation.

4. How much of a problem is synthetic identity fraud for your organisation?

Free initial assessment to help you quantify the problem

We'd like to offer you a free retrospective data test to help unmask the presence of Synthetic Identities across your portfolio, so that your organisation can ring-fence suspicious accounts, run further investigations and prevent fraudsters from obtaining further credit.

Predictive analytics to identify risk factors and flag suspicious accounts

Retrospective data testing serves as proof of value and supports the development of customised fraud models and/or attribute append services, ensuring alignment with your requirements.

We will model the customer identity information you were provided with at onboarding alongside our own more detailed UK customer record data, (a near complete account of UK adult population data with 3 billion customer records, over 70 data sources and covering over 1000 different attributes) and will use predictive analytics to identify high risk factors for synthetic identity and flag suspicious accounts.

A fraud model, tailored to your needs

We begin by discussing your specific needs. During the data testing process, we will use a sample of your historical application data (including known genuine and fraudulent examples) to train a fraud model, tailored to your fraud prevention objectives. The data attributes necessary for model development are covered in our data test guidelines and consultation summary document, which will be supplied to you upfront.

The fraud model leverages our extensive and trusted datasets and determines which will be the most valuable attributes to offer actionable insights for your fraud investigation teams. We furnish up to 1000 attributes that enable you to examine each individual and transaction closely, supporting improved decision-making. This appended data is shared securely with you, for analysis.

As part of our deliverables, we will also provide you with a Fraud Score and Fraud Risk Band.

Depending on your requirements and configuration, we anticipate that creating a custom model build and completing a retro test will take between 6-8 weeks, following receipt of your sample data and confirmation of its compliance with data test standards by our Data Science team.

For attribute append-only services and returning data, we estimate a turnaround time of 3-4 weeks to deliver the data back to you.

Contact us today to organise your free,
no obligation data test on 029 2067 8555
or email ukenquiry@lexisnexis.com
risk.lexisnexis.co.uk

LexisNexis®
RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.