
FAKE IDENTITIES,
REAL THREAT:
FIGHT BACK AGAINST SYNTHETIC ID
emailage®
The Email Risk Score Company

What is synthetic ID fraud?

In the past, synthetic ID fraud was a tactic used by consumers with poor credit ratings. Back then, it was also known as a "credit bust out" with the goal to open credit card accounts or apply for loans, then default and move on. Now, fraudsters have discovered the same tactics, and are using them at scale to cause major headaches in almost every industry for businesses of all sizes.

Synthetic identity fraud occurs when fraudsters use a blend of real and fake information to create a "new" individual. In some cases, the information used is entirely fake. The bad actors will open up new credit cards or auto loans under the fake individual's name, with the goal of creating credit records and boosting the credit profile.

Why has it become the new go-to tactic for fraudsters?

"There is no "victim" in synthetic ID fraud. There is no real person to make a complaint. It takes a bit more time for a fraudster to create the ID, but it has a much bigger payoff"

- Brett Johnson, former fraudster

While synthetic ID fraud is not a new strategy for fraudsters, it has become a new favorite. The shift to EMV has pushed fraudsters to card-not-present fraud and new application fraud, which is directly correlated to synthetic ID fraud. This shift along with large scale data breaches that have resulted in millions of identifying records becoming readily available on the dark web have brought fraudsters back to this tried and true method.

3 ways Fraudsters Synthesize an ID

Legitimate SSN + Fake Name

"Inactive" SSN + Real Name

(Typically a Child or someone who has died)

Fabricated SSN + Fake Name

What's worse, there are ways to speed up this process. Fraudsters now will "piggyback" onto a legitimate cardholder's account as an authorized user. How is this accomplished? Using social engineering tactics, fraudsters convince unsuspecting victims that if they can add them as an authorized user to an existing bank or credit card account, they'll make deposits in order to use the account. In reality, fraudsters have now created a synthetic ID attached to a real account with a very real credit history.

Although fraudsters would have you believe that Synthetic ID fraud is a victimless crime, the truth is there's a hefty price to be paid for it, usually paid by creditors and retailers. After fraudsters open new lines of credit or get loans approved, they frequently default on them. This kind of fraud can be especially difficult to detect because one of the natural risks of the credit and lending business is that even good customers can default. That makes it especially critical to detect fraud before applications are processed in order to prevent unnecessary defaults. Defaults are accompanied by lost revenue from payments not made to creditors or retailers, in addition to lost product, and fraud dispute fees.

A serious financial threat

The growth of synthetic ID fraud shows few signs of slowing. Easy access to data used by fraudsters to create synthetic IDs will continue to make fraud an attractive option.

According to studies conducted by the Aite Group, credit card losses that resulted from synthetic ID fraud topped $820 million in 2017, an increase of 17% from the previous year. Forecasters expect this to grow to $1.3 billion by 2020.

This shift requires a more sophisticated approach to predicting and assessing risk, as well as a more holistic approach to fraud management.

Here's how to fight back

Analytics-based solutions can combat synthetic ID fraud by delivering insight that detects linkages and suspicious patterns, which help determine if an applicant is a real person.

These models leverage advanced keying logic to validate components of an applicant's identity beyond the social security number. Keying technology drives down the number of false positives that normally accompany fraud products, by looking at all of the data used to make a digital identity. This includes more traditional static data such as name, phone number, social security number, and physical address. It can also include newer pieces of dynamic data like IP address, geolocation, device identifiers, and email address.

The most sophisticated solutions provide information that helps determine if there are inconsistencies with the applicant's behavior across a consortium of data or if the application has high-risk variables that are known to be predictive of fraud.

Step one:

Determine your exposure

When most people think of sleeper cells, images of spy thrillers and international intrigue are what come to mind. In the world of fraud management, sleeper cells consist of accounts that are intentionally aged (or 'farmed') lend an air of credibility, which is of course required to carry out synthetic ID fraud.

Fraudsters know that you have controls based on the tenure of an account. In order to outflank these controls, they create accounts then "sit" on them for enough time to appear legitimate.

That time could be 3 months, 6 months, or even a year for the most dedicated fraudsters. They know that the longer an account is aged to appear real, the higher the potential profits from their attacks will be. The actual amount of time will be based around how much they have tested your control points. And you can bet they have tested them much more than you are aware of.

At the end of the day, they are attempting to give you an impression that these accounts represent "good customers" with tenure, so your controls become irrelevant. That's why it pays dividends to determine your fraud risk exposure. How much could you lose to an attack launched by these sleeper cells?

Determine your average fraud loss, per account.

The key here is to determine the percentage of accounts that are potential sleeper cells, or otherwise "at risk" based on tenure.

Think of it this way: If your average loss is USD $2,000 and .5% of your account portfolio is at risk (let's call it 100 accounts), losses represent a staggering USD $200,000.

Food for thought: the Association of Certified Fraud Examiners estimates that organizations suffer annual fraud losses equal to 5% of their revenues.

Takeaway: Determine the answers to the following:

- What are your current losses?
- How much could you lose to synthetic ID fraud?
- What would be the business impact of a fraud attack?
- How would fraud impact sales, operations and finance?

Step two:

Define good behavior

It's likely that fraudsters know your business just as well as you do. They know that you utilize several controls based around the tenure of the account and are aware that you expect fraud to happen in the first few months that an account exists.

If you want to stay a step ahead of them, consider merging your tenure controls with transaction value. This means that simply having an account that's six months old, with minimal activity, should not be automatically cleared. Instead, these accounts should still be considered new or risky.

Think of tenure as something closely associated with significant transaction amounts. For example, if an account has existed for six months and has USD $5,000 in transactions associated with it, then it can be considered legitimate.

Combining account tenure with a meaningful transaction amount and positive payment history constitutes a control that is very hard for fraudsters to replicate. This way, you can select your trustworthy population and segment it against the rest of your transactions. Then you can reduce controls and focus on accounts that are potentially risky.

Takeaway: Define which customers are truly your good customers through analysis of:

- Tenure
- Confirmed Activity
- Good behavior

Step three:

Always plan one step ahead

Fraud trends continually evolve, so your fraud management strategy must do the same to stay ahead of the curve. There is no "silver bullet" in fraud prevention. No vendor will solve all of your problems, no matter what they may promise.

A prudent approach is to stay current, continuously optimize and never think you have your controls adjusted to "good enough" because complacency is exactly what fraudsters are counting on.

Don't be afraid to consistently evaluate your vendors and fraud solutions by constantly calculating the incremental value. What type of ROI are you seeing from the solutions you utilize? Typically, financial teams like to see a 3x ROI, at minimum.

Takeaway: Test your controls, & test them frequently.

- From time to time, be sure to evaluate the efficiency and accuracy of every solution you deploy. Solutions should evolve as quickly as fraud trends.
- Run periodic quality assurance tests. Ensure that all your rules are firing properly and be sure you have redundancy built into your systems.
- Don't let attempts escalate into successful attacks.

Where Emailage comes in

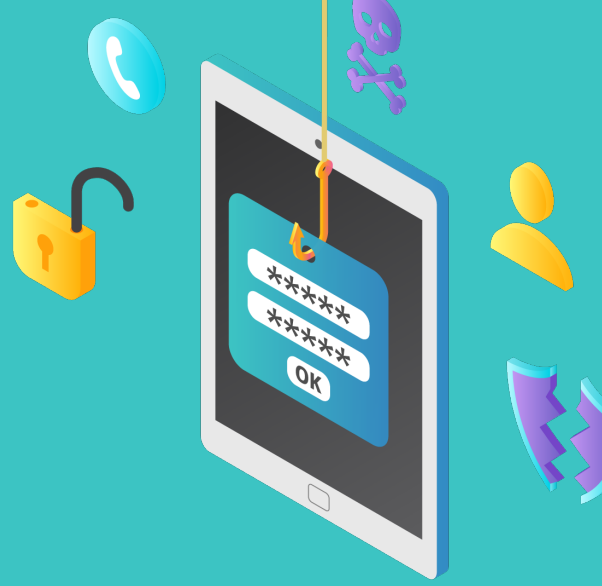
There's one key piece that fraudsters need to successfully commit synthetic ID fraud: an email address. To identify potential synthetic IDs, we use crowdsourced network intelligence to look for behavior changes around the use of the email address in transactions.

We help combat synthetic ID fraud by delivering insights that detect linkages and suspicious patterns, which help determine whether or not an applicant is a real person.

Our predictive EmailRisk Score uses email address metadata as the core for transactional risk assessment and identity validation. Our online identity profiles fuse this data with other elements, such as a phone number, address and customer name.

Using the data analysis from our consortium of confirmed fraud data, our EmailRisk Score sets up rules-based automation that will help you approve the lowest risk applicants and decline the highest risk applicants quickly and automatically. This leaves only your most at-risk or murky applications for manual review.

Emailage also offers custom modeling through machine learning. Using advanced machine learning, shared data, and your specific business practices and customer data our decision scientists create custom risk models that make your fraud detection even more efficient. These models are updated on a weekly basis, evolving as quickly and quietly as the fraudsters attacking your bottom line.



Conclusion

Fraudsters aren't going to stop attacking businesses any time soon, so there's really no time to waste when addressing synthetic IDs. Criminals are highly motivated to innovate their approaches as rapidly as possible, and it's important to implement a solution that addresses the continued rise of synthetic IDs from multiple engagement points while continuing to evolve with the threats it fights.

Fortunately, robust and reliable countermeasures to synthetic ID fraud are available to organizations. With these solutions, organizations can quickly, reliably and affordably identify suspicious activity to help mitigate risk without encumbering legitimate consumers with unnecessary checks.

Checklist: Steps to Stopping Synthetic ID Fraud

Synthetic ID fraud is a real threat and fraudsters are turning to it more as EMV chips and multi-factor authentication make other traditional fraud attacks more difficult. While implementing a full proactive fraud management solution can be lengthy and complex, there are steps you can begin taking immediately to stop these attacks.

Preparation:

Taking steps to proactively fight fraud is critical, but before you can solve the problem, you must understand the problem. The following steps will help you evaluate your company's baseline fraud costs and goals, making protecting your customers easier.

- ☐ **Identify your fraud exposure** - Understanding how high your risk factor is for fraud will help identify flaws in your current prevention systems.
- ☐ **Review account set up & change processes** - Identify the data collected when accounts are created and when contact information is changed. This information will help with evaluating fraud prevention solutions and data analysis.
- ☐ **Calculate current fraud costs** - Understanding current fraud losses, attacks, and costs will allow you to understand the problems your business is facing and make educated decisions about how to best lower those costs.
- ☐ **Assess your current fraud prevention strategy** - What is the hit rate? How much are you paying versus how much is it saving you? Understanding your current investment into fraud prevention, if you have one, will help you understand whether or not your current vendors are meeting your needs and where gaps should be filled.

Implementation:

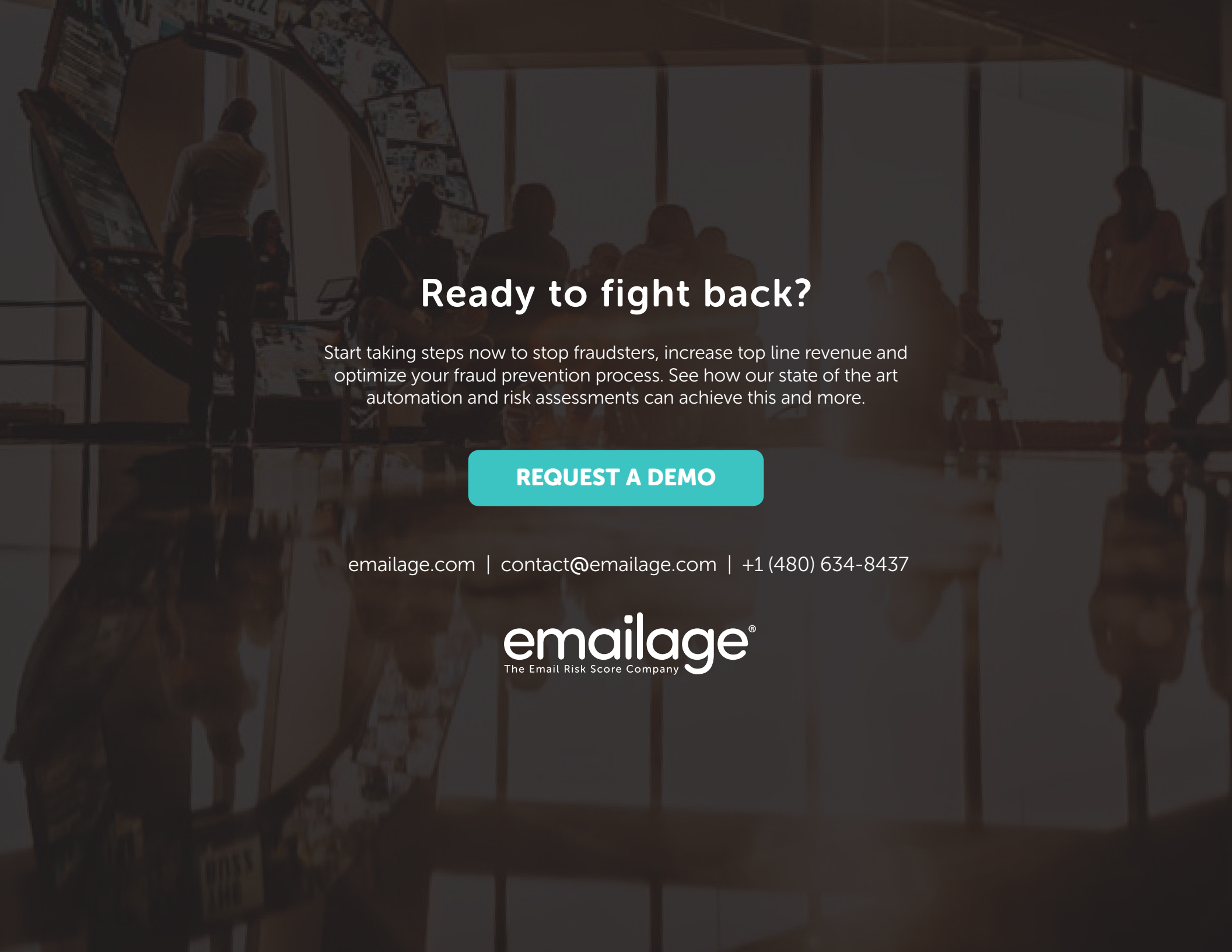
After creating your baseline documentation, you will have a deeper understanding of what problems your business faces and how to best solve those problems. You will also be able to create goals for stopping fraud, such as reducing customer friction and increasing top line revenue.

- ☐ **Create internal blacklists** - Maintaining a database of email addresses, names, and phone numbers that have been associated with fraud in your system is the first step towards preventing those fraudsters from coming back. You can also share this confirmed fraudulent data with your solution provider to enhance shared network intelligence.
- ☐ **Leverage external data** - Internal blacklists are a start, but because they are static and do not contain external data they can only go so far. Work with a fraud prevention solution provider to leverage third party data and shared network intelligence to detect elements of synthetic IDs that have been used in previous fraud attacks.
- ☐ **Utilize multi-factor checks** - Synthetic identities are often created with a mixture of real and fake elements. Don't rely on a single point of data to detect it. Work with a solutions provider that can analyze multiple data points such as social security number, address, email address, and IP address location.
- ☐ **Embrace automation** - Fraud management solutions will allow you to create rules for declining very high risk and approve vert low risk transactions and applications automatically. This will leave your manual review team diving into only necessary accounts and create a more frictionless experience for your legitimate customers.

Moving Forward:

The work of fraud prevention doesn't stop when you've launched your new fraud prevention strategy and implemented the new vendor stack. A holistic, proactive approach requires some post-launch maintenance.

- ☐ **Mind your ROI** - Since you had a good grasp on your baseline costs and impacts of fraud loss, after your strategy and solutions have been active for a few months you need to go back and calculate your return on that investment. Are your vendors meeting your expectations and their promises to you?
- ☐ **Calculate new baselines** - If you are implementing a fraud strategy for the first time, you may have had forecasts or potential impacts calculated but no tangible data to create baselines. Now that your new strategy is working for you, fill in the gaps in your starting data. Knowing these baselines will help you audit your solutions in the future.
- ☐ **Start employee awareness training** - Synthetic ID fraud is often accompanied by social engineering tactics used to age accounts or gain access to legitimate identities. Now that you have automated solutions in place, patch up the weakest link in any financial fence–humans. Periodic employee security awareness training will help your people spot and stop social engineering tactics adding another layer of security to your investment.



Ready to fight back?

Start taking steps now to stop fraudsters, increase top line revenue and optimize your fraud prevention process. See how our state of the art automation and risk assessments can achieve this and more.

REQUEST A DEMO

emailage.com | contact@emailage.com | +1 (480) 634-8437

emailage®
The Email Risk Score Company