Slipping through the cracks: How synthetic identities are beating your defenses

Introduction

In 2014, ID Analytics recognized a fundamental shift in the frequency and sophistication of synthetic identity attacks, reporting a significant increase in the rate of synthetic fraud over the previous three years,[1] and the magnitude of synthetics continues to grow. Industry analysts state there were $800 million in losses from synthetic identity fraud through credit cards alone in 2017 and predict these losses could skyrocket to 1.2 billion by 2020.[2] Today, it is the fastest-growing and hardest-to-detect form of identity theft in the United States.[3]

These statistics demonstrate that synthetic identities are successfully circumventing enterprises' defenses during account opening and lurking in lenders' portfolios waiting to strike.

ID Analytics conducted a study to (a) examine how synthetic identity behaviors find their way past fraud and credit screening at leading financial institutions (FIs), and (b) determine indicators for isolating likely synthetics. This study is part one of a synthetic research series that examines synthetic behaviors and how deeper insight into identity and consumer intention can be used to help reduce the growth of this elusive problem.

Synthetics study – quantifying the problem and identifying indicators

ID Analytics' study quantifies the number of synthetic identities bypassing lenders' risk assessments and demonstrates the differences in behavior between synthetic identities and other types of fraud or credit abuse. The results uncover indicators which demonstrate how synthetics circumvent third-party fraud and traditional credit risk solutions, emphasizing the need for a purpose-built strategy to help enterprises maintain a strong defense against this rising threat.

Synthetic identity fraud is breaking through enterprises' defenses

Based on ID Analytics' research, between 85-95% of applicants identified as potential synthetic fraud (as defined by the FIs included in this study) were not flagged as high risk by traditional fraud models built to predict the potential of third- party fraud (including identity theft). See Figure 1.

When we analyzed synthetic fraud from a credit perspective, the majority of synthetic identities (tagged by the FIs included in this study) fell within the category of good, very good, or excellent credit based on the FICO scoring model. Depending on where enterprises set their credit limits, this could allow many synthetics to successfully pass credit underwriting processes. In fact, more than half of synthetics in this example were identified as having good, very good, or excellent credit (see Figure 2).

Figure 1. Synthetics are not being flagged as high risk

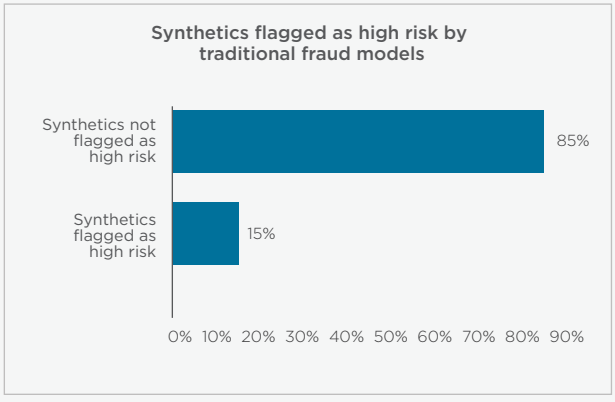
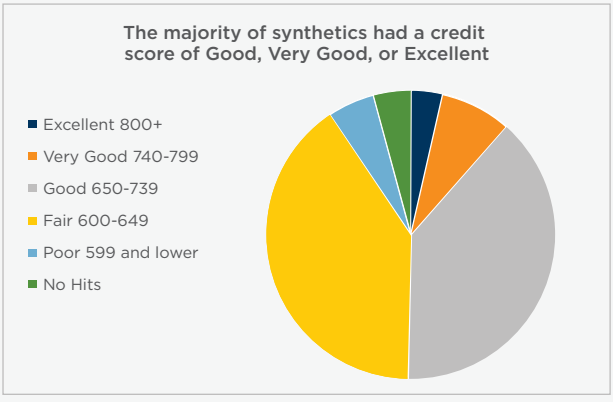


Figure 2. Synthetics are breaking through credit and fraud defenses



As the figures above demonstrate, tools built to help reduce identity fraud and risky credit behaviors that enterprises have traditionally used at account opening are vulnerable to synthetics. Synthetic identities are infiltrating enterprises during account opening and doing considerable financial damage; this elusive nature of synthetics has led to the dramatic increases in losses from synthetic identities over the past several years.[4]

How can enterprises be better prepared to target these fraudsters? The second part of this study examined the differences between traditional third-party fraud and credit risk behaviors and those of synthetic identities to develop an understanding of how synthetics are eluding these otherwise highly effective risk screening processes.

Behavior comparison: Synthetic identities vs. traditional third-party fraud

Synthetic identities have had success making their way through enterprises' defenses because their patterns of behavior differ from those of identity thieves, which most origination systems are built to identify.

Third-party fraud, or identity fraud, occurs when a legitimate identity is stolen and used to access new credit services. These fraudsters work to obtain as much credit and as many services as possible and max out the credit line and service value quickly, before the victim discovers they have been compromised and reclaims their identity. From an identity information perspective, these fraudsters will often utilize a victim's stolen core identity elements such as their Social Security number (SSN), name, and date of birth and swap in new contact information (such as phone and address).

Synthetic fraud, however, occurs when fraudsters create a fictitious identity, then establish credit by opening one account, then others at multiple businesses as they build a positive payment history. They often nurture these identities over time to maximize the potential pay-off. It could be years before they bust-out a credit line resulting in a loss to the enterprise they have targeted.

Synthetics pass fraud checks because they profile themselves differently than traditional fraud. ID Analytics' research uncovered traits that are highly indicative of third-party fraud and synthetics (see Figure 3). When examining certain traits including velocity, pattern verification, and confirmed negative behavior, the differences in behavior between third-party fraud and synthetics become indicators for enterprises regarding the type of fraud they are dealing with.

Figure 3. Behavior traits across third-party and synthetic fraud.

Traits of Fraudulent Behavior	Third-Party Fraud	Synthetic Fraud
Velocity – how fast is the identity seeking credit?	More indicative	Less indicative
Pattern Verification – anomalies in identity elements and consumer behavior	Less indicative	More indicative
Confirmed Negative Behavior - past fraud association	More indicative	Less indicative

These differences in critical traits make it important for enterprises to develop their fraud strategies based on the behavior of synthetic identities and not rely solely on solutions built to detect the potential of third-party fraud.

Behavior comparison: Synthetic identities vs. traditional credit bads

From a credit perspective, synthetics develop their own credit history, rather than steal it from a consumer victim. This portion of the study reveals the different patterns synthetics use to develop their credit histories and subsequently go bad, when compared to legitimate consumers with bad credit.

Traditional credit scores are designed to assess the creditworthiness of an applicant, specifically the risk of the applicant defaulting on a credit responsibility. Synthetics bypass credit defenses because they have success building good credit scores, which they achieve through a variety of ways, that allow them to hide their true intent – to misuse credit.

On average, identified synthetics have a comparable number of tradelines and time on file to the overall population of credit applicants. However, the impact of the identified synthetics is more severe due to over-utilization on credit lines and the rapid speed at which they build up that utilization once they decide to bust-out. ID Analytics' research shows that one year after the time of application, synthetics had an average amount past due of more than $8,000, (approximately 4 times higher than the identified credit bad population).

ID Analytics isolated intentional misuse behaviors at the time of application by examining patterns that led to extreme credit abuse outcomes. When examining likely synthetics or individuals who are planning to intentionally misuse credit, our research found the following behaviors to be highly indicative of an applicant's intent to misuse credit:

- Amount Owed: the utilization of credit and how much an individual owes is representative of how they plan to use new tradelines
- Unique Tradelines: the types of accounts an individual possesses, or the lack of certain accounts can speak to the intention of an applicant
- Life Stability: the increased permanence around an individual decreases the likelihood that an individual will intentionally misuse credit

By placing heightened importance on these behaviors, enterprises can improve their ability to identify synthetics and other consumers with the likely intent to misuse credit – strengthening credit defenses against a challenge that has vexed underwriting systems for years.

Conclusion

Synthetic identities are one of the more challenging fraud patterns to detect and prevent because their methods, behaviors, and outcomes are so diverse. As a result, enterprises often have a different view of whether synthetic identities are an underlying fraud problem or a credit problem making this issue even more difficult to solve.

As demonstrated in our study, synthetic identities behave differently than traditional third-party fraudsters and consumers whose credit has gone bad. The following are guidelines that enterprises may want to consider in order to help detect synthetic identities:

- Leverage solutions which are purpose built to assist in detecting synthetic identities
- Take a holistic approach – avoid solving for a portion of the problem by identifying a wide range of synthetic identities and potential credit abuse
- Fight synthetics on your terms – whether you view synthetics to be a fraud or credit problem, acquire solutions and build strategies which attack these fake identities as your enterprise experiences them

Synthetic identities manifest themselves in different ways within an enterprise, and without the ability to effectively fight the problem as each organization experiences them – be it fraud or credit risk – many lenders and service providers are stuck in neutral against this rapidly growing threat.

ID Analytics continues to learn more about the evolving threat of synthetic identities, as discussed here and in forthcoming research. We have used this insight to develop and release new solutions designed to address the threat of synthetics.

To learn more about how ID Analytics can help you tackle synthetic identities head-on, contact us at sales@idanalytics.com or visit our website at www.idanalytics.com.

[1] ID Analytics, October 2014, *The Long Con: An Analysis of Synthetic Identities*.
[2] Payments Journal, http://paymentsjournal.com/the-business-of-synthetic-identities/ (accessed September 28, 2018).
[3] *CNBC*, https://www.cnbc.com/2018/06/07/scammers-create-a-new-form-of-theft-synthetic-identity-fraud.html (accessed September 28, 2018).
[4] *Digital Transactions*, https://www.digitaltransactions.net/with-synthetic-id-fraud-losses-soaring-complications-beset-a-search-for-solutions/ (accessed October 12, 2018).