All synthetic identities are not created equal: Examining purported synthetic signatures

Introduction

Synthetic identity fraud is the fastest-growing type of financial crime in the United States.¹ As revealed in part one of the ID:A Labs synthetic identity research series, because synthetic identities manifest themselves in multiple ways and often appear to be legitimate consumers, they are extremely effective at circumventing traditional risk defenses. ID Analytics has been researching and tracking synthetics for years to better understand synthetic fraud behaviors and develop solutions that help enterprises protect consumers and their businesses from this mounting threat.

Part one of ID:A Labs synthetic identity research series, Slipping through the cracks: How synthetic identities are beating your defenses uncovered that 85-95% of applicants identified as potential synthetic fraud were not flagged as high risk by traditional models built to predict third-party fraud (i.e., identity theft). The study demonstrated how differences in behavior between synthetic identities and other types of fraudulent or high-risk credit applicants are allowing synthetics to successfully bypass lenders’ fraud and credit risk assessments. In this installation, ID:A Labs examined the variability in behavior of synthetic identities and how those differences make synthetics very difficult to solve with solutions that target only one signature trait associated with the crime.

Synthetic identity signals

As synthetic identities have become increasingly common and the need for effective defenses more critical, risk managers have been drawn toward solutions which target specific “tricks of the trade” associated with fake identities. In the past few years several methodologies and signals have been associated with synthetic identities, including credit piggybacking, taking advantage of social security number (SSN) randomization, and targeting faceless channels.

Credit piggybacking, or the addition of an authorized user to an already established credit account, has perhaps been the behavior most commonly identified as a signature trait of synthetic identities, and certainly the one that most synthetic solutions target today. This practice is often legitimately used by parents to build their children’s credit scores. However, criminals exploit this process by paying strangers with good credit to add synthetic identities to credit card accounts which quickly builds their associated credit scores. These criminals may not abuse the credit lines they have been added to, but instead use the synthetic identities’ artificially created credit scores to apply for new products. Fraudsters can then nurture these accounts, sometimes for years, before maxing out the credit lines and disappearing without a trace.

ID Analytics has spoken at length about another synthetic signal – potentially randomized SSNs. In 2011 the Social Security Administration (SSA) began randomizing the issuance of SSNs, which changed the way criminals were able to build synthetic identities. Prior to this, fraudsters either used a stolen SSN or they made one up, which risk analysts were often able to detect. After the SSA’s change, criminals were able to make up an SSN from the range of numbers not issued prior to 2011 and have a number that appeared legitimate without stealing an identity. Eight years after the change, enterprises continue to find it difficult to distinguish between legitimately issued randomized SSNs (which include those issued to immigrants and individuals born after 2011) and fictitious numbers being asserted by fraudsters who are taking advantage of the new system.

Digital channels are popular with legitimate consumers, but they can also be considered a signal of synthetic identities. The logic is straightforward; given that synthetics have no real person behind them, in-person channels are mostly off-limits which makes digital channels an appealing avenue of attack for this crime. Unlike credit piggybacking and potentially randomized SSNs, the use of digital channels is too widespread to be the main focus of synthetic solutions. Therefore, if an applicant displays other common synthetic signals and has applied for credit or services through a digital channel, this may be used by risk managers as a confirming trait of a suspected synthetic applicant.

No silver bullet: An analysis of synthetic identity signals

As enterprises increasingly adopt solutions and rule-based strategies which target these supposed signals, ID Analytics wanted to better understand how ubiquitous these traits truly are among synthetic identities. ID:A Labs analyzed known synthetic identities, as identified by leading financial institutions, to determine the frequency and variability of credit piggybacking, the exploitation of randomized SSNs, and the use of digital channels.

The analysis uncovered that while each of these signals are common among synthetic identities, none captured a meaningful majority of the fake identities. The study found that credit piggybacking was employed by synthetics nearly 50% of the time, randomized SSNs were used by synthetics almost 40% of the time and that faceless channels were the preferred choice for slightly more than 50% of the identified synthetic identity fraud cases (see Figure 1).

Conclusion

Over the past several years, synthetic identities have seen a precipitous rise at U.S. lenders and service providers. The urgency to find solutions to this challenge has led many enterprises to adopt solutions which target specific behaviors thought to be the signature traits of synthetic fraud. This study highlights the risk of relying on a silver bullet to combat synthetic identities. While synthetic identities have some common traits, not all synthetics are created equal making the problem difficult to detect through solutions targeting a single high-risk behavior.

ID:A Labs continues to learn more about the evolving threat of synthetic identities, and the final chapter of our research series will delve into the validity of a more holistic approach for combating synthetic identities which focuses on overall identity legitimacy and intention. Building models and strategies to assess such an elusive target is no easy task, but as the next brief will illustrate, ID Analytics’ research and development of synthetic solutions demonstrate that it is not impossible.

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.