Fraud methods for identifying synthetic identities in credit applications and portfolios

Identifying trends and solutions to confirm “proof of life” based on alternative data.
Table of contents

Executive summary ........................................................................................................................................ 2
Confronting the harsh realities of synthetic identity fraud ................................................................. 3
The importance of tracking identity emergence .................................................................................. 5
Defending against synthetic fraud in underwriting .............................................................................. 7
Differentiated “beyond credit data” strategy ...................................................................................... 9
Conclusion .............................................................................................................................................. 11
Executive summary

The recent surge in efforts to reduce account takeover fraud has led to an increase in synthetic identity fraud. Synthetic identities are a means for fraudsters to steal funds by inventing false identities that are not connected to true living consumers. These fraudsters curate identities, which then transact with financial institutions and other lenders, eventually “busting out”. Since credit data is manipulated to create these identities, it is challenging to detect and prevent synthetic fraud using credit data alone.

LexisNexis® Risk Solutions has identified many “proof of life” data signals based on alternative data, focusing on a holistic view of identity development and maintenance including:

- **Identity emergence**: The patterns by which an identity is created and logged in the credit workflow
- **Identity consistency**: The patterns by which identity elements are consistent or inconsistent with other identity elements on file
- **Identity transactions**: The patterns by which an identity develops and evolves over time
- **Identity crowding**: The patterns by which other identities develop at the same time and location as a target identity

LexisNexis Risk Solutions is well positioned to help lenders and other users of identity verification and fraud data better understand these patterns that result in financial loss.
Confronting the harsh realities of synthetic identity fraud

Defining synthetic fraud

Fraud based on synthetic identities has accelerated in recent years. The scheme involves creating false identities from scratch that transact with financial institutions, mobile phone providers, insurers and government tax agencies. These identities enable fraudsters to steal from target institutions and/or enable consumers with poor credit history to qualify for more generous credit terms.

Invented identities rarely correspond to true credit-active consumers, or even with an actual living consumer. As we will see, lenders need deep insight into the emergence of identity behavior to best detect this type of fraud.

While it is relatively easy to define, it can be challenging to clearly identify a synthetic credit applicant among true identity applicants using traditional credit bureau-based fraud and verification approaches. In most cases, a synthetic identity uses fictitious information like name, SSN, address, phone, etc., to establish and register a new identity with the credit bureau, taking advantage of existing loopholes in credit reporting systems. This can be accomplished in several ways, such as reactivating a deceased consumer’s identity that is not being actively monitored or stealing a minor’s identity information before the minor enters his or her data into the credit system. As we will see, lenders need deep insight into the emergence of identity behavior to best detect this type of fraud.

Market trends

Lately, fraud activity has soared, with lenders reporting just under $28 billion in total fraud losses in 2016. While the impact of synthetic fraud is more difficult to quantify, it is estimated to be a significant and growing driver of total losses industry-wide. Since EMV chips have made account takeover more challenging and less profitable for fraudsters, application fraud has become the path of least resistance for fraudsters. A survey of card issuers revealed that they are anticipating new account fraud/application fraud to spike in the wake of EMV. The proliferation of “at a distance” mobile and online credit products also make it easier for fraudsters to engage in the credit system through online channels without engaging in hard-to-compromise actions like obtaining a voter registration or drivers license. These online channels afford fraudsters with opportunities to experiment and fine-tune their fraud schemes with little chance of arrest at a point of purchase or point of application.
Based on LexisNexis Risk Solutions research and customer interviews, several factors are responsible for this increase in synthetic fraud as a preferred mode of stealing from financial institutions, telecommunication providers, auto lenders and similar companies:

**Data breaches and EMV adoption**: The frequency and scope of significant consumer data breaches coupled with the full-scale U.S. adoption of EMV technology has made traditional “stolen credit” schemes more difficult, riskier and less profitable. Consumers and lenders are becoming far more sensitive to these sorts of frauds and more actively work to prevent them, forcing fraudsters to explore other avenues to defraud banks.

**SSN randomization**: The introduction of SSN randomization in June 2011 has made it more difficult for U.S. banks to assess the authenticity of consumer applications; fraudsters have seized upon this opening to create a CPN (credit privacy number) that can be used as an SSN proxy. For example, prior to randomization, SSNs included information about the state of issuance, date of issuance and even if an SSN could have been issued. The legitimacy of an SSN, and consistency checks between SSN data and place of issuance and the age of the consumer, are no longer effective verification tools to identify manufactured identities established after 2011.

**Lack of consumer victim**: Typical stolen identity fraud includes a victim who will eventually alert banks and credit reporting agencies to initiate anti-fraud activity such as account closures and credit blocks within hours, days or weeks of fraud occurrence. Synthetic identity fraud has no true consumer victim to raise a red flag. As a result, the fraud stops only when the synthetic identity busts out and is detected by the victimized institution. Since the bust out looks like a legitimate low-risk consumer who stops paying, these frauds are often misclassified as credit defaults. As a result, they are often not included in typical fraud programs based on verified and tagged fraud performance.

**Underwriting policy**: As both credit underwriting and account management practices are streamlined to reduce customer friction, they are also becoming more remote via online and mobile channels. These streamlined “at a distance” capabilities provide a forum for fraudsters to create and curate identities electronically with reduced risk of apprehension.
The importance of tracking identity emergence

The current state of the consumer credit industry has greatly aided the accelerating proliferation of synthetic identity fraud. With the large number of new identities reported to the credit bureaus each year and a significant number of identities associated with multiple SSNs, the identity climate is predisposed to confusion and manipulation.

Fraudsters take advantage of the complicated identity climate to manipulate and curate new identity information through the facilitation of an emerging synthetic identity in the credit system. Research by LexisNexis Risk Solutions shows that between six and seven million new U.S. identities were reported by the credit bureaus every year from 1995-2016. These new identities are mostly maturing teens and immigrants entering the credit system. This value has been relatively steady over this time period (See Figure 1). With this steady influx of emerging identities, there is an opportunity for synthetic identities to hide among legitimately emerging younger consumers and immigrant populations.

Figure 1: Change in # of new identities seen by LexisNexis Risk Solutions has been relatively constant since 1995
Fraudsters understand the credit bureau reporting ecosystem and have become increasingly adept at operating within its confines to exploit various entry points to breed synthetic identities. A typical emerging identity can be seen first at a variety of sources: at a credit bureau as they obtain their first credit card; auto and/or student loans; at voter registration point; or at drivers license facilities. One sign of an increased risk of synthetic identity fraud is that emerging identities are increasingly first reported by a credit bureau more often than other hard-to-compromise sources such as drivers license or voter registration rolls.

The trend here is startling—there is a dramatic increase in credit bureau-sourced emergence reaching 800% year over year growth in 2015 (Figure 2), starting shortly after U.S.-based SSN randomization in June 2011. Neither birth rate nor immigration rate can fully account for this influx of new identities that are first reported by credit bureaus since the overall emergence of identities is relatively constant in this period (Figure 1). While it is difficult to isolate the source of this credit bureau trend, one possible hypothesis is an influx of synthetic identity emergence. Accordingly, LexisNexis Risk Solutions actively monitors identities and identity emergence patterns to examine these types of high-risk identity trends. This report includes many recommendations based on the findings of these data efforts.

**Figure 2: Change in proportion of identities that are first seen on credit files has ballooned since 2012**
Defending against synthetic fraud in underwriting

Today’s consumers demand a seamless and prompt application and account origination experience. Consumers readily abandon processes encumbered with too much friction and overhead, resulting in lost revenue opportunities for lenders and other service providers. Financial institutions and retailers must straddle an ongoing and delicate balance: meeting customer expectations for a frictionless experience while protecting against fraud with fortified protocols. By missing the signs of an application association with a synthetic identity, an institution exposes itself to unrecoverable losses. Combining a streamlined customer experience with strong fraud defenses designed to snare synthetic identity remains an ongoing challenge.

Recent internal studies at LexisNexis Risk Solutions leveraged advanced analytics approaches such as machine learning and data mining, precise identity linking and consumer intelligence to uncover a profile of characteristics commonly associated with a synthetic identity.

The best, and in reality, the only opportunity to proactively uncover a synthetic identity attempt and prevent the synthetic identity from entering a customer portfolio is to include fraud checks at the time of account origination. Recent internal studies at LexisNexis Risk Solutions leveraged advanced analytics approaches such as machine learning and data mining, precise identity linking and consumer intelligence to uncover a profile of characteristics commonly associated with a synthetic identity. The studies identified a clear association between the lack of proof of life indicators, the length of time the identity had been established and the absence of authenticated connections between different pieces of the identity, including SSN, address, phone and government-issued identity documents.

Identity elements

The process of generating a synthetic identity is based on fraudsters manipulating identity data within the credit system. The key to establishing proof of life is to examine identity details that exist outside of the information within a consumer’s wallet. These proof of life insights typically occur as part of a consumer’s day-to-day transactions across a broad range of credit and non-credit activities. However, by
examining the broader emergence of identity files, the behaviors of identity files and the coherence of identity data, clear identity trends emerge:

**Identity emergence:** Identity emergence refers to the method, source profiles and identity elements of consumers that appear in the LexisNexis Risk Solutions identity system. Often there are clear patterns of consumer emergence consistent with synthetic identities. These emerging patterns lead to a variety of key questions related to whether the identity emerged in a way expected of a true identity:

- Do they emerge from sources that are very similar to credit bureau sources (such as utility records) or from official public record sources such as courthouses?
- Do their relatives emerge in a similar way?
- How do they transact with their identity as they emerge; do they appear overly curated in their emergence approach?
- Are the identity elements of the emerging consumer consistent across family members?
- Have the identity elements been used before?
- Have we seen identity elements co-occurring in the past, with similar or new identity elements?

LexisNexis Risk Solutions can help lenders assess these questions.

**Identity consistency:** By examining how any identity elements like SSN, name, address and phone have transacted in the past, a fraud analyst can review new identity information being appended to a record. The analyst can then determine whether this information has been seen with this identity, which sources have reported the identity information and which identities have been associated with this information in the past. By examining the consistency of the identity, we can examine the use and reuse of SSNs, addresses and phone numbers, as new identity information is associated with existing information. Anomalies here are often evidence that synthetic identity (or some other identity theft event) is occurring.

**Identity transaction behavior:** Emerging identities that are curated by bad actors for the purposes of fraud typically behave very differently from those that are authentic files. For example, most legitimate emerging files apply for credit rather sparingly, however, curated files tend to apply for credit quickly with the purpose of building credit profiles in a short time for fraudulent purposes. While thin file consumers may apply for a single auto loan or credit card and manage their limited credit for an extended period, curated synthetic identities tend to build more quickly, attempting to rapidly build a thick file that would qualify for increasing loan amounts on their way to bust out. One word of caution—synthetic identities can occur on longer timelines than other types of fraud because there is no victim to report identity compromise. As a result, it is important for fraud analysts to review longitudinal behavior to capture identity transformations over time horizons that are longer than typical for other fraud schemes.
Identity crowding: Identity crowding occurs when identity information is reused multiple times across emerging identities. In particular, it is common to see fraudulent identities coming through single addresses. In one case, we have observed an address from which over 10,000 new identities emerged. These identities then tend to “move to” less crowded addresses where they then engage in fraud. Since these addresses are dependent on fraudster control, this sort of trend can be a common indicator that suspicious behavior is occurring. It is not uncommon for similar crowding-type patterns to occur for other identity behavior including phones or national identifier. As a result, it is important to track address usage and crowding, including cases where common addresses have secondary range addresses (like apartment number) missing and/or reused.

Differentiated “beyond credit data” strategy
To make informed identity assessments, it is important to possess a complete and holistic view of identity development and usage over time. LexisNexis Risk Solutions aggregates identity data across a variety of different credit and non-credit sources. By combining these sources, users of the identity repository get a full picture revealing how identities emerge and transact with other identities. Rather than depending on a single view of U.S. identities at the root of many less effective approaches used today, LexisNexis Risk Solutions compiles identity records from thousands of sources to create a more robust and effective full-identity resource for identity management. These sources can be summarized into four general categories:

Credit bureau identity data: All three national credit bureaus are monitored for all the identity events that most financial institutions report during their normal business activities. Monitoring credit bureau identity information exposes both new identities when first reported by financial institutions in addition to changes to existing identities, for example change of address. Differences in identity information reported by the credit bureaus can also identify high fraud risk conditions, especially if only a single credit bureau reports an identity or piece of identity information or if there are unique variations of identity elements appearing at one or more of the credit bureaus. Credit bureau data often shows the first signs of synthetic emergence when fraudsters register synthetic identities designed to defraud financial institutions.
**Government reported identity activity:** LexisNexis Risk Solutions evolved from 40 years of experience in gathering government reported public record data sourced from over 2,400 county courthouses and all 50 state governments. Among the document types assembled are real estate property deed transfers, county property tax records, court judgments, felony and criminal convictions, tax liens, evictions, occupational licenses, drivers licenses, vehicle and watercraft registrations, voter registrations, bankruptcy filings and related records. Tens of millions of identities that have no financial records are found in these government and court sources. These sources are difficult to manipulate or falsify and provide strong proof of life credentialing against attempts to create synthetic identities or manipulate existing ones.

**Utility and phone identity activity:** LexisNexis Risk Solutions monitors identity activity reported by landline phone carriers, utility reporting agencies and other phone directories to track confirmed address changes in near real-time. This dimension provides a very timely source of address changes and current residential status as well as presenting identity coverage on millions of U.S. consumers who are credit invisible. Since identity emergence requires contact information, it is fairly common for phone sources to show early signs of synthetic identity emergence.

**LexisNexis search activity and Fraud Defense Network (FDN):** There are more than 3,000 institutions who use LexisNexis identity authentication services, including large financial institutions, regional branch banking institutions, auto lenders, retail merchants, online merchants, payment service providers, mobile phone carriers, public utilities and dozens of other industries that require identity due diligence on their customers. This search activity provides vast insights for detecting suspicious behavior associated with synthetic and other forms of identity fraud. The real-time nature of search activity allows lenders to quickly detect patterns of rapid succession and variations in identity activity used when attempting to open accounts. Those who partner with LexisNexis also receive access to unique and high-quality proof-of-life verification elements only available with access to LexisNexis® FDN event activity data. LexisNexis monitors millions of authentication events per day to search for evidence of suspicious or fraudulent identity misuse, such as addresses with unusual identity activity or SSNs that are suddenly shared by multiple new identities. While very useful in identifying criminal fraud ring activity, these identity queries also provide insight into normal changes in identity information over time.
Conclusion

The rise of synthetic identity fraud illustrates how successful fraudsters have become at compromising the reliability of traditional credit reporting systems. Verifying an applicant using a narrow view of consumer activity alone can significantly weaken fraud defenses. Our study found that identities reported by only a single credit bureau are 10 times more likely to be synthetic than identities reported by all three credit bureaus. Expanding an identity authentication strategy beyond historical methods to include alternative data such as public records and government-issued documents can support a more comprehensive applicant perspective and highlight identity anomalies. By broadening this perspective, lenders and other organizations assessing fraud risk gain a broader picture of identity, identity emergence and identity transactions to more effectively isolate identities likely to be synthetic.

Building a better understanding of the information included on the application and separately reviewing key elements of the related identity can help highlight hidden risks that may not readily stand out in an initial onboarding review. By individually analyzing the application components, LexisNexis data can help detect high-risk conditions like search velocity, correlations between the application elements being reported together, common data points like address, phone or SSN shared by multiple identities and more. The next step is to scrutinize the application identity against a diverse set of characteristics that can also uncover irregularities such as number of sources on file or lack of corroborating sources, frequent name or address changes, number of relatives and suspicious associates. Finally, we evaluate the correlations and relationships between the application information and the related identity, providing deeper intelligence that speeds the discovery of applications presenting a higher risk for fraud and warrant deeper investigation.

Implementing a holistic view of identity emergence, consistent transactions and crowding can dramatically reduce identity fraud. By applying a full range of identity data from LexisNexis Risk Solutions, lenders can weaken synthetic identity attempts at the source of origination. This type of fraud thrives on inconsistencies and tenuous connections that can often be discovered by analyzing the identity associated with the application. Adding a multifaceted authentication protocol can help snare an invalid identity element that is often missed or mistakenly overlooked in the rush to preserve the customer experience. By combining risk visibility with deeper, multi-sourced content, it is possible to magnify inconsistencies that signal a synthetic identity and mitigate the threat before the application is approved. These strategies can aid in preventing damaging fraud losses from impacting your portfolio by working in sync to help eliminate the loopholes enabling synthetic identities to proliferate.

LexisNexis Risk Solutions can design a fraud defense strategy that helps your business balance escalating customer expectations with extensive fraud defenses, combining an unmatched level of identity expertise and high-value verification intelligence leveraging proprietary data sources and analytics.
Contact us to learn more about implementing a risk-based strategy that easily adapts to evolving market conditions and supports accelerated customer onboarding.

For more information, call 866.858.7246 (U.S.) or 029 2067 8555 (UK) or visit lexisnexis.com/risk/financial/fs-fraud-detection-prevention.aspx

1 Nilson Report, October, 2016
2 Aite, “Financial Institution Fraud Trends,” March 2017
4 LexisNexis Labs®, May 2017

About LexisNexis® Risk Solutions
At LexisNexis Risk Solutions, we believe in the power of data and advanced analytics for better risk management. With over 40 years of expertise, we are the trusted data analytics provider for organizations seeking actionable insights to manage risks and improve results while upholding the highest standards for security and privacy. Headquartered in metro Atlanta USA, LexisNexis Risk Solutions serves customers in more than 100 countries and is part of RELX Group plc, a global provider of information and analytics for professional and business customers across industries. For more information, please visit www.lexisnexisrisk.com.

This white paper is provided solely for general informational purposes and presents only summary discussions of the topics discussed. This white paper does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their attorneys, compliance departments and other professional advisors about any questions they may have as to the subject matter of this white paper. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Copyright © 2017 LexisNexis. All rights reserved. NXR11596-00-0817-EN-US