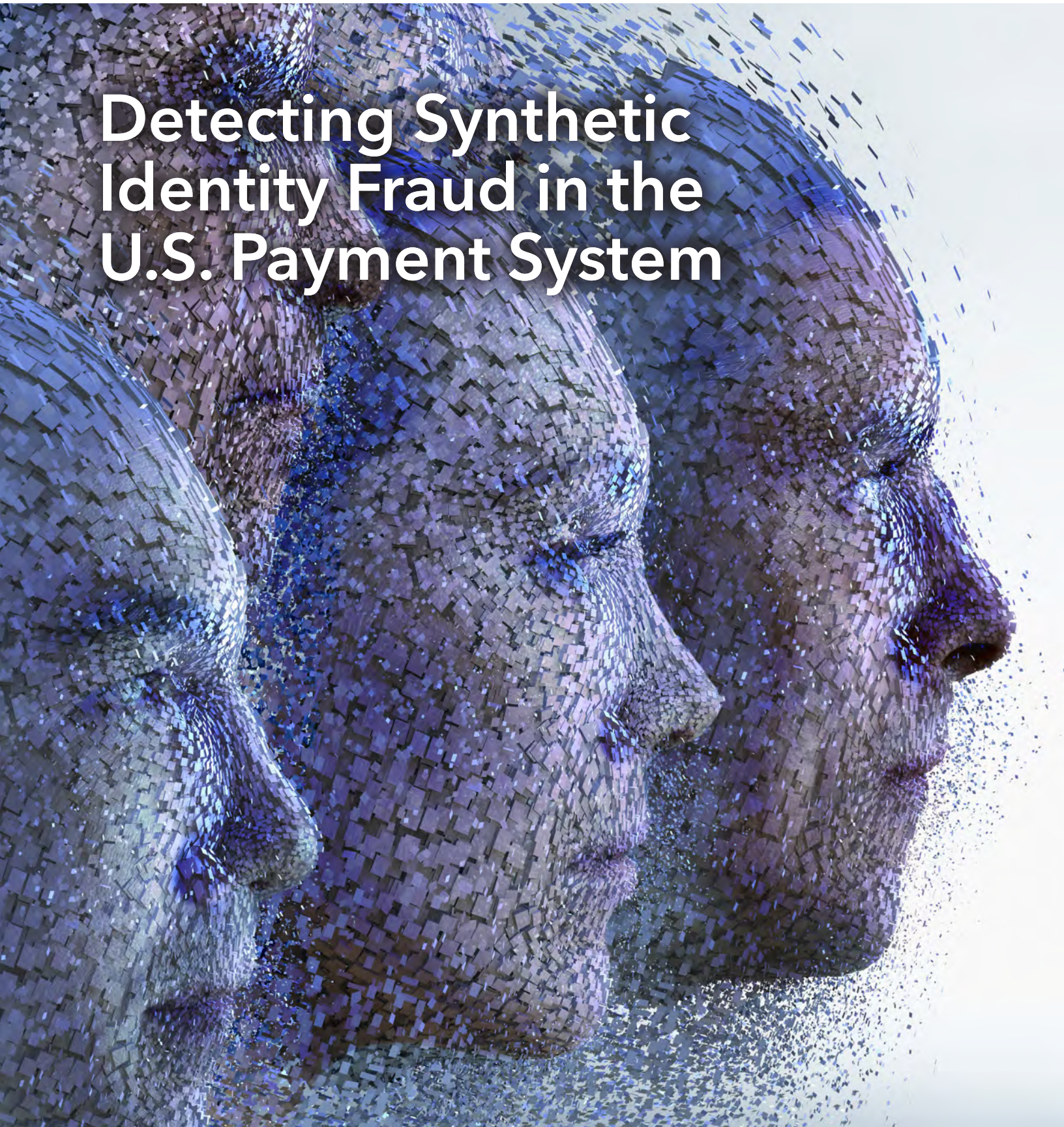
THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

PAYMENTS FRAUD INSIGHTS
OCTOBER 2019

Detecting Synthetic Identity Fraud in the U.S. Payment System



FOREWORD

Table of Contents

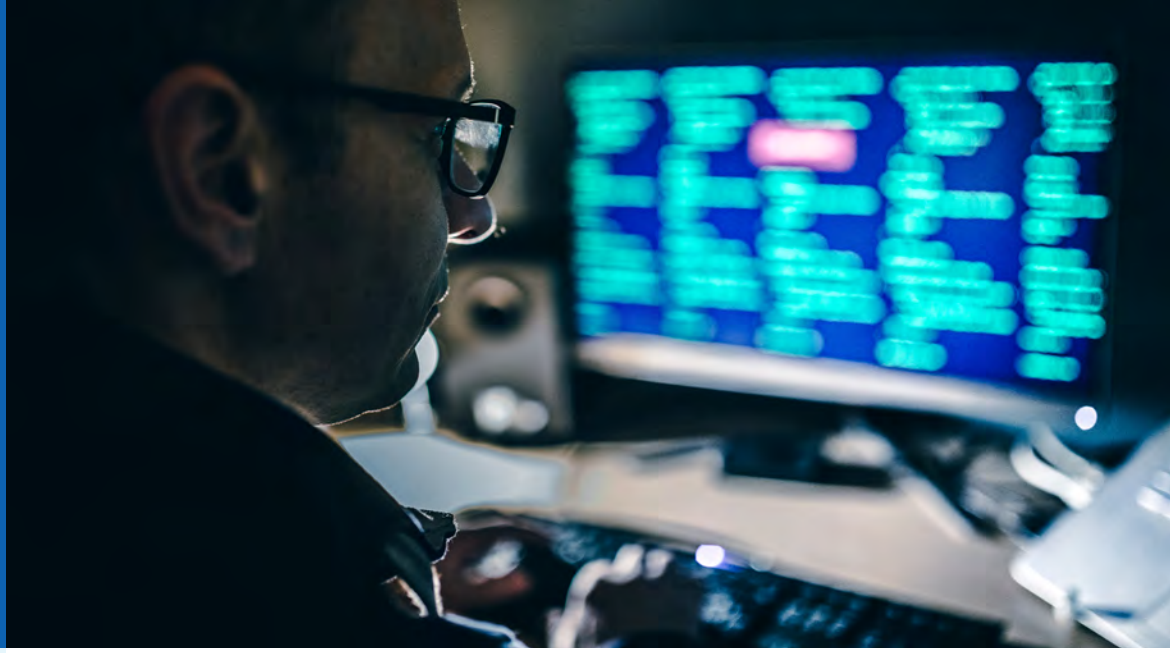
In 2018, the Federal Reserve launched an initiative to raise awareness and encourage action against synthetic identity payments fraud, reportedly the fastest-growing type of financial crime facing the United States. In July 2019, we published our first *Payments Fraud Insights* white paper, *Synthetic Identity Fraud in the U.S. Payment System*, which focused on causes and contributing factors.

This white paper takes our work a step further by exploring the detection of synthetic identities. It highlights how financial institutions and other payments stakeholders analyze and connect multiple data points on individual account holders and across all accounts in their portfolios to identify behavior trends. In addition, it points to the importance of connecting with other industry and law enforcement stakeholders to effectively prevent and mitigate synthetic identity fraud.

The Federal Reserve, in collaboration with the payments industry, is working toward a vision of faster, more secure and efficient payments in the United States – which includes this and other outreach efforts. Synthetic identity fraud is not a problem that any organization or industry can tackle independently, given its far-reaching effects on the U.S. financial system, healthcare industry, government entities and consumers. Likewise, our *Payments Fraud Insights* white papers are informed by the knowledge of many subject matter experts and Federal Reserve colleagues. We thank you for your insights and look forward to continued dialogue and collaboration as we work to reduce synthetic identity payments fraud.

Jim Cunha
Secure Payments and Fintech Division Head
Senior Vice President, Federal Reserve Bank of Boston

HIGHLIGHTS FROM OUR FIRST WHITE PAPER

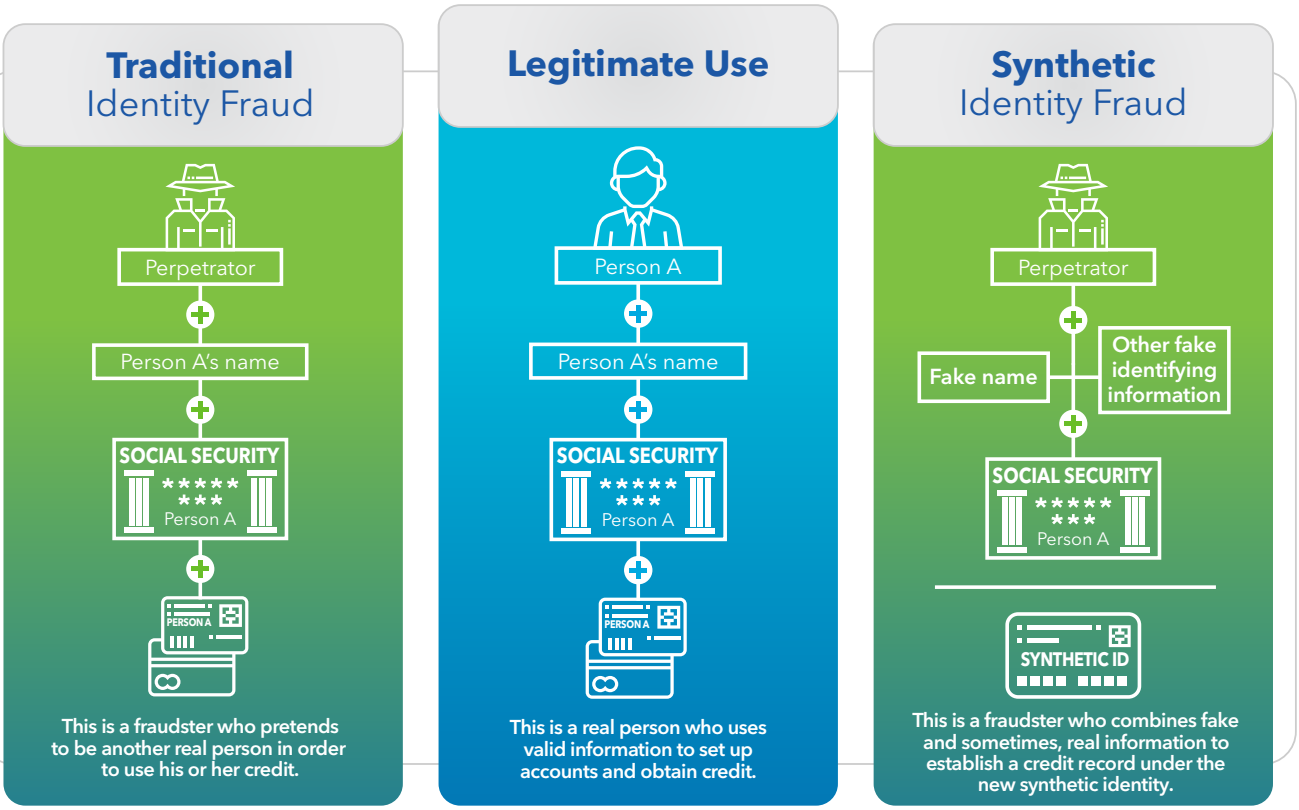


Synthetic identity fraud occurs when perpetrators combine fictitious and sometimes, real information, such as names and Social Security numbers (SSNs), to create new identities – which then may be used to defraud financial institutions, government agencies or individuals. It is difficult to measure the full impact of this type of fraud in the U.S. payment system due to differing definitions and approaches to detection. Auriemma Group estimates that synthetic identity fraud cost U.S. lenders $6 billion and accounted for 20% of credit losses in 2016.

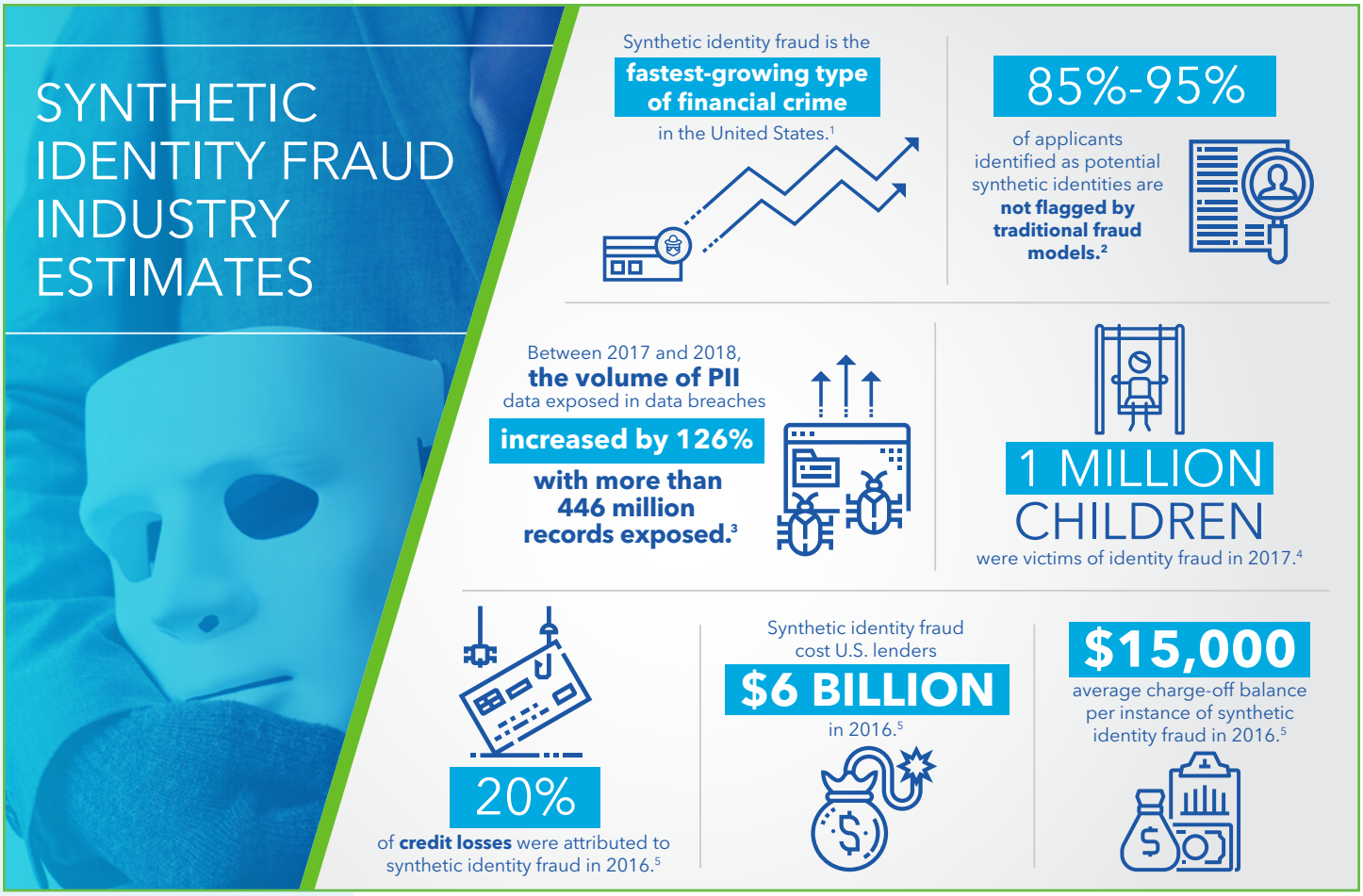
As described in our first white paper, *Synthetic Identity Fraud in the U.S. Payment System*, synthetic identity fraud is difficult to detect and often unreported. Fraudsters leverage the personally identifiable information (PII) of individuals – such as children, the elderly or homeless – who are less likely to access their credit information and thus, discover the fraud. Synthetic identities can behave like legitimate accounts and may not be flagged as suspicious using traditional fraud detection models. This affords perpetrators the time to cultivate these identities, build positive credit histories, and increase their borrowing or spending power before "busting out" – maxing out the line of credit with no intention to repay. Fraudsters can employ a variety of tactics to multiply their payouts. One such tactic is for the fraudster to claim identity theft on the fictitious identity, allowing charges to be reversed and credit lines reopened.

Synthetic identity fraud differs from traditional identity fraud, where a fraudster pretends to be another real person and uses his or her credit. Traditional identity fraud is typically detected and reported more quickly because the victim notices unusual charges on his or her financial statements.

DIFFERENTIATING TRADITIONAL IDENTITY FRAUD FROM SYNTHETIC IDENTITY FRAUD



The ease and low cost of creating synthetic identities contributes to the widespread impact of this type of fraud on the financial, insurance and healthcare industries, government agencies and consumers. Sophisticated crime rings can leverage multiple tactics at scale to cultivate synthetic identities, including using fake addresses, creating sham businesses and forming relationships with collusive merchants to cash in.



Industry experts point to the following as key contributing factors leading to increased synthetic identity fraud:

- **Near-universal use of SSNs as identifiers in the United States.** The Social Security Administration (SSA) created SSNs to track an individual's earnings and benefits. SSNs have evolved into a principal way that private industry and government agencies identify people and assess their legitimacy. Compounding the difficulty of determining if an individual is real, the SSA began randomizing the assignment of SSNs in 2011. This eliminated the geographical significance of the first three digits (also called the area number) and, in turn, the predictable, chronological significance of the remaining digits.

1 Excerpted from "Fighting back against synthetic identity fraud", January 2019, McKinsey & Company, www.mckinsey.com. Copyright © 2019 McKinsey & Company. All rights reserved. Reprinted by permission.
2 ID Analytics (2019). *Slipping through the cracks: How synthetic identities are beating your defenses.*
3 Identity Theft Resource Center (2019). *2018 End-of-Year Data Breach Report*
4 Javelin Strategy & Research (2018). *2018 Child Identity Fraud Study*
5 Auriemma Group (2017). *Synthetic Identity Fraud Cost Banks $6 Billion in 2016*

The ease and low cost of creating synthetic identities contributes to their widespread impact.

- **Increase in PII available to fraudsters.** According to the Identity Theft Resource Center, the volume of PII exposed in data breaches increased by 126% between 2017 and 2018 to more than 446 million records exposed. Dark web marketplaces sell these breached records, including bank account login credentials, driver's licenses, credit card numbers and SSNs. Experian reports an SSN costs fraudsters as little as $1, and it's just $30 for an individual's full identity package of name, SSN, birth date, account numbers and other data.
- **Credit process gaps.** When a fraudster initially uses a synthetic identity to apply for credit at a financial institution or retailer, the entity sends an inquiry to one or more credit bureaus. The bureau creates a credit profile for the synthetic identity, which helps legitimize its identity even when credit is denied. The fraudster also can manipulate the credit ecosystem through piggybacking – adding a synthetic identity as an authorized user on an account belonging to another individual with good credit. In many cases, the synthetic identity acquires the established credit history of the primary user, rapidly building a positive credit score.

HOW SYNTHETIC IDENTITIES ARE USED IN PAYMENTS FRAUD

DETECTING SYNTHETIC IDENTITIES

Financial institutions employ Know Your Customer (KYC) processes and other tools to gain reasonable assurance of a customer's identity. These checks help fulfill legal, regulatory and internal policy requirements to limit financial institution risks. Fraudsters seek to pass KYC tests by making synthetic identities appear valid. This includes fabricating identification credentials, social media profiles and other documentation. Some fraudsters apply for credit in person to make it appear that the synthetic applicant must be real. In fact, a study conducted by ID Analytics indicated that only half of synthetics apply for credit using digital channels. This underscores the need to be vigilant, even when financial institutions have strong customer identification programs and can verify an applicant in person.

Fraudsters seek to pass KYC tests by making synthetic identities appear valid.

Many U.S. regulatory controls applicable to detecting and identifying synthetics are rooted in the Bank Secrecy Act (BSA), the primary anti-money laundering law in the United States. BSA requires financial institutions to properly identify customers, maintain appropriate financial transaction records, and report suspicious activities to government agencies. The USA PATRIOT Act amended the BSA to support information sharing and investigations into suspected money laundering and terrorism financing.

The Customer Identification Program (CIP) Rule implements the requirements of Section 326 of the USA PATRIOT Act and requires financial institutions to know the identity of each customer. At a minimum, financial institutions must collect a customer's name, date of birth, address, and SSN or taxpayer number before opening an account. The SSA introduced the Consent Based Social Security Number Verification (CBSV) service in 2008 to enable paid subscribers to verify a SSN holder's name and date of birth. CBSV can help financial institutions comply with CIP, though the SSA currently requires written confirmation from the SSN holder.

This verification usually takes several days, so legitimate customers can find it inconvenient – particularly as technology advances enable automated account decisions and allow near-instantaneous approval. In June 2020, the SSA expects to roll out an electronic CBSV service[6] pilot program to allow companies to electronically check an individual's name, SSN and date of birth against the SSA database. Industry stakeholders and subject matter experts express optimism that the electronic CBSV service will help financial institutions and other payments stakeholders balance compliance with customer expectations of fast credit approvals.

Technology can improve data analysis efficiency and effectiveness, enhance security, reduce operational costs – and help detect synthetics.

Technology can improve data analysis efficiency and effectiveness, enhance security and reduce operational costs. It also can help detect synthetics. Institutions can leverage artificial intelligence and machine learning to determine expected customer behavior patterns and detect anomalies that potentially indicate fraud. As fraud tactics continue to evolve quickly, these tools need frequent recalibration to remain effective. Furthermore, automated lending processes may need adjustment and updates, since they can provide another avenue for fraudsters to receive credit. For example, a synthetic with a high credit score could be targeted by an institution's marketing campaign and receive a pre-approval offer for a new account.

6 As a result of Section 215 of the Economic Growth, Regulatory Relief and Consumer Protection Act.

SYNTHETIC IDENTITY CHARACTERISTICS

Financial institutions and other payments stakeholders can find value in going beyond verifying static identity elements by looking for unusual recurring patterns and relationships between transactions to detect potential synthetic identities. Examples include multiple account applications from the same IP address or device, or assigned to the same name, SSN or physical address. These checks also help identify indicators of possible fraud networks – for example, individuals without a common city or surname who appear as authorized users on multiple accounts.

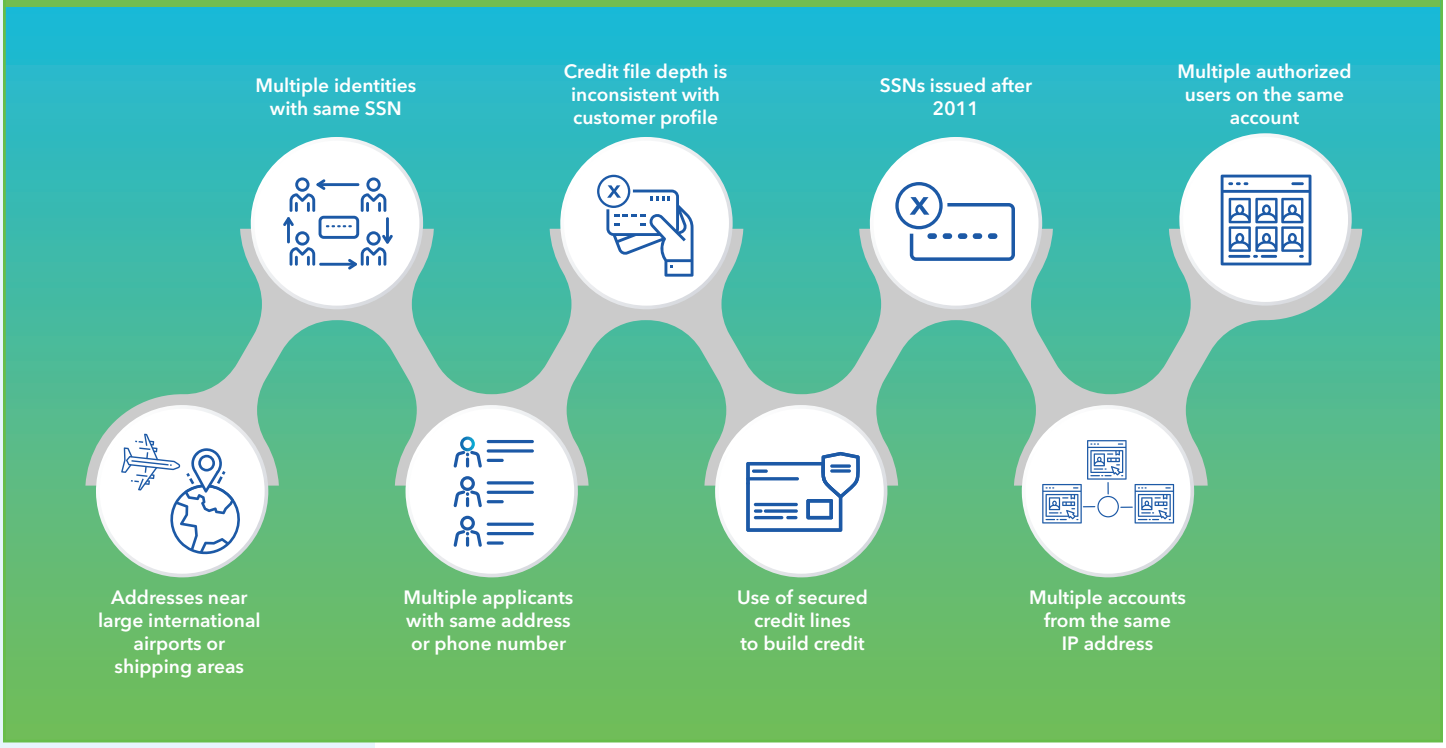
According to a study by ID Analytics, fraud models built to predict traditional identity fraud did not flag 85% to 95% of potential synthetic identity fraud applicants. Often, the tactics used to cultivate synthetic identities differ from those used to perpetrate traditional identity fraud. For instance, synthetic identity fraud takes place over a longer period, as fraudsters open multiple accounts to build a positive credit history for the synthetic and maximize their eventual payoff. Traditional identity fraudsters must move more quickly because they know they are likely to be detected faster. Other differences include anomalies in identity elements and consumer behavior.

Synthetic identities reportedly are more likely to appear first when applying for credit (in other words, they initially appear in a credit bureau report), rather than when associated with other life events, such as a birth or applying for a driver's license. LexisNexis found that the number of new identities first reported by a credit bureau has increased dramatically since randomization of SSNs began in 2011,

and rose by 800% in 2015. Over that same period, the overall number of new U.S. identities – factoring in the birth rate and immigration – remained relatively constant, indicating a potential increase in synthetic identities. A synthetic identity that first appears via a credit bureau is likely to have anomalies in its identity elements, such as a 40-year-old applicant with a brief six-month credit file.

That said, focusing solely on one particular characteristic could lead to false positives. Looking only at the length of a credit history could unnecessarily disadvantage or deny credit to certain types of legitimate customers – such as immigrants and formerly impoverished or incarcerated people who only recently gained access to credit. This underscores the importance of aggregating multiple data sets and connecting multiple customer characteristics to more effectively detect synthetic identities.

COMMON CHARACTERISTICS OF SYNTHETIC IDENTITIES



SLEEPER SYNTHETICS

Once synthetics enter a lender's portfolio, detection becomes increasingly difficult because they initially look and behave like normal customers. Synthetic identities can be nurtured for months – and sometimes, years – to achieve higher credit limits. Fraudsters cultivate accounts by making small purchases and paying them off to build good repayment histories. Before a bust-out occurs, these sleeper accounts help add credibility to a synthetic identity to boost its borrowing and spending power. According to TransUnion, the average charge-off rate for likely synthetic identities within a given lending portfolio is less than 30%. This implies that 70% of suspected synthetic identity accounts are temporarily exhibiting typical consumer payment patterns – making them more difficult to detect.

Synthetics initially look and behave like normal customers, as they are nurtured for months – and sometimes, years – to achieve higher credit limits.

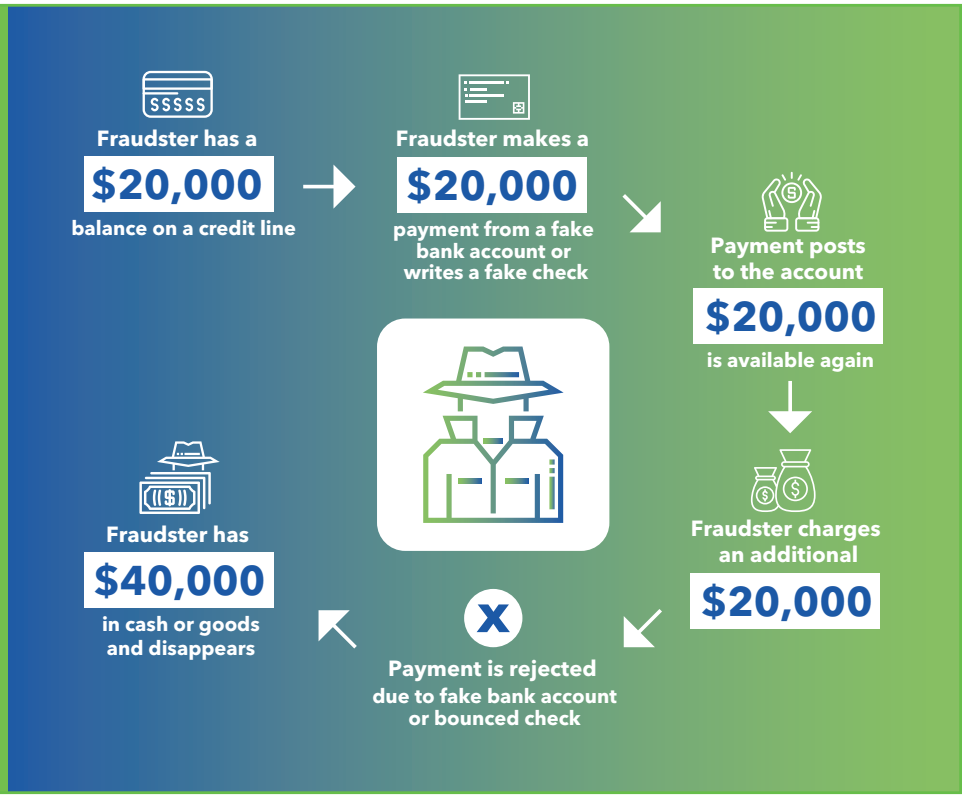
Sleeper accounts also can be used to support the validity of other synthetic identities. For example, dozens of individuals can be authorized users on the same credit card. This is a potential indicator of synthetics piggybacking on one another.

DETECTING SYNTHETICS IN BUST-OUTS

Often, a financial institution may not identify an account holder as synthetic until after a fraudster busts out and the collections team is unable to find a real person to pay the debt.

Busting out is not always a one-time event. For example, fraudsters sometimes multiply their payouts by claiming they were subject to identity theft to convince financial institutions to reverse charges and reopen credit lines. Experts suggest a 2017 Federal Trade Commission (FTC) rule change eliminating the need for a police report when claiming identity theft may have contributed to a growth in consumer disputes. This rule change makes it easier for consumers – and thus, fraudsters – to dispute information on trade lines, which are the credit accounts on a credit report.

SYNTHETIC IDENTITY BUST-OUTS: MAXIMIZING THE PAYOUT



Additionally, fraudsters know that banks and credit bureaus have limited time to review fraud disputes due to requirements of the Fair Credit Reporting Act. Fraudsters can take advantage of this window and flood the financial institution with an overwhelming number of claims to reduce the likelihood that the institution will have time to conduct a full investigation before the deadline. This prevents disputed information from negatively affecting the synthetic identity's credit report.

Fraudsters know that many financial institutions establish dollar-value thresholds and automatically settle any fraud claims below that figure. These policies are in place to reduce the operational cost of investigations and promote a positive, seamless customer experience for legitimate account holders. Fraudsters can attempt to avoid detection by determining an institution's threshold and disputing transactions in increments just below it.

Another ploy is to take advantage of the time required for a payment to clear. This time varies by financial institution. Under this strategy, fraudsters max out their credit and pay off the card balance with fraudulent checks or stolen or invalid bank account information. Once the card balance returns to zero, but before the payment clears, the fraudster maxes out the credit line again with no intention to repay.

HOW FRAUDSTERS MAXIMIZE THEIR PAYOUTS

Claim identity theft

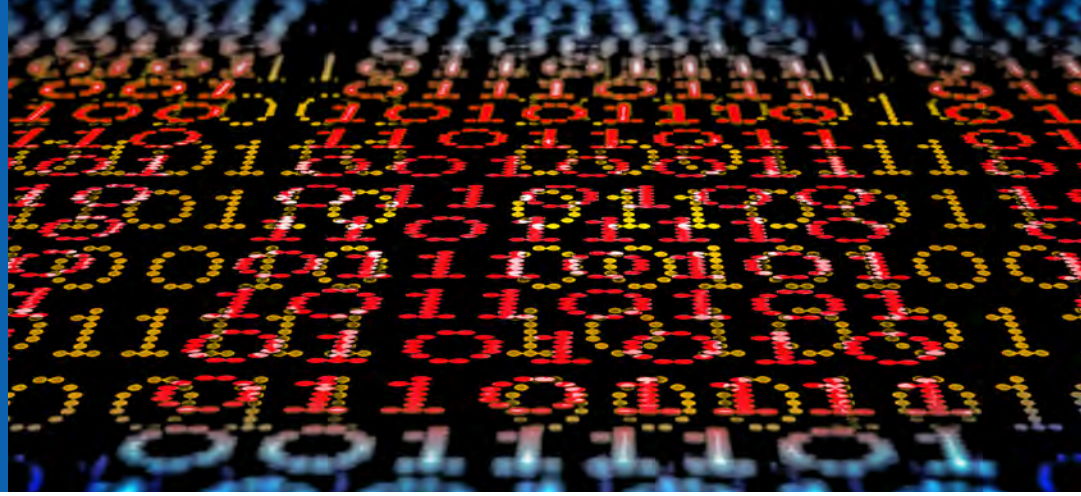
Use fake checks

Pay with invalid or stolen bank accounts

Initiate chargebacks

Initiate a credit bureau dispute

CATEGORIZING THE LOSS



Financial institutions generally bear the losses caused by bust-outs. Financial losses due to synthetic identity fraud often are incorrectly categorized as credit losses, as the synthetic identities appear on the surface to be actual non-paying customers. Inconsistent categorization is exacerbated by a lack of common industry definitions and classification for synthetic identity fraud.[7] In addition, when an institution attempts to collect funds from the synthetic identity, there is no real person to find – and it may not be considered cost-effective to investigate further.

It is important to categorize losses correctly. If a financial institution flags synthetic identity fraud activity, it can use the information to track linked accounts (e.g., other accounts with the same SSN, name, address, etc.) or other associated identities. If incorrectly flagged as a credit loss, the credit bureaus remove the delinquency after seven years and the fraudsters can attempt to re-use the same synthetic identity to rebuild credit and bust out again.

CATEGORIZING THE LOSS AFTER A BUST-OUT

Fraud Loss?

- Goods/services received
- No intention to repay
- Fraudster busts out using synthetic identity tactics

Is the account holder real or fake?

Credit Loss?

- Goods/services received
- Promise to repay
- Customer defaults when financial circumstances change

7 The Federal Reserve is leading an effort with industry stakeholders to develop a Fraud Classification Model for Payments to promote consistency in fraud reporting, initially for ACH, wire and check payment types.

THE IMPORTANCE OF INFORMATION SHARING

To address the growing problem of synthetic identity fraud, payments and fraud experts indicate a need for greater awareness of its scope and scale, as well as additional information sharing across the payments industry. As payments stakeholders share more information about trends, behaviors, threats and best practices, they can improve the industry's collective synthetic identity fraud detection and mitigation practices.

As payments stakeholders share more information about trends, behaviors, threats and best practices, they can improve fraud detection and mitigation practices.

Information sharing is particularly important for smaller financial institutions, which may not have the same technology or personnel resources as larger companies. Collaboration can help stakeholders aggregate and analyze data on synthetic identity fraud – and smaller financial institutions and other stakeholders report these collaborative partnerships to be successful. Industry collaboration can be a key step toward identifying trends and developing strategies to reduce specific fraud vulnerabilities.

Ongoing collaboration between law enforcement and financial institutions also is vitally important to share information about threats and trends and support effective investigations. The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury, whose mission is to safeguard the financial system through the collection, analysis and dissemination of financial intelligence. FinCEN manages information-sharing processes enabled by the USA PATRIOT Act. Section 314(a) of the Act allows law

Many payments and fraud industry experts believe the benefits of information sharing across the industry outweigh any perceived drawbacks.

enforcement agencies to request information from participating financial institutions for terrorism or money laundering investigations, while Section 314(b) allows participating financial institutions to share customer information with one another in support of their own due diligence, compliance and reporting requirements.

However, financial institutions may remain hesitant to share information with other industry stakeholders. While laws and regulations require companies to report certain suspicious behaviors related to money laundering and terrorism financing, they are not usually required to provide the same information about losses attributed to fraud. Financial institutions may fear losing a market advantage by revealing too much to competitors about their practices. They also may be concerned about reputational risk, data privacy and security requirements. Despite these challenges, many payments and fraud industry experts believe the benefits of information sharing across the industry outweigh these perceived drawbacks.

CONCLUSION

No single organization can stop wide-ranging, fast-growing synthetic identity fraud on its own. Fraudster tactics continually evolve to stay a step ahead of detection – and the most sophisticated fraudsters can operate at scale in organized crime rings, generating significant losses for the payments industry. It is imperative that payments industry stakeholders work together to keep up with the evolving threat posed by synthetic identity fraud, which includes anticipating future fraud approaches.

The industry is taking steps to create new fraud models and use advances in technology, such as artificial intelligence and machine learning, to help mitigate synthetic identity fraud. Fraud detection innovation is key, as experts indicate most traditional identity fraud tools are ineffective at detecting synthetic identity behaviors and characteristics.

Financial institutions and payments stakeholders should take a comprehensive and collaborative approach as they continue to improve their fraud detection capabilities. More specifically, stakeholders can benefit from developing consistent definitions for synthetic identity fraud, analyzing multiple data sources and characteristics beyond static PII elements, identifying commonalities and relationships between identities, and sharing behavior and trend information with other industry participants.

The Federal Reserve's next white paper in the *Payments Fraud Insights* series will explore approaches to mitigating synthetic identity fraud, as we continue our efforts to raise awareness and explore payments improvement opportunities.

For more information, visit FedPaymentsImprovement.org and submit or update your FedPayments Improvement Community profile and select "Payment Identity Management" as a topic of interest.

THE **FEDERAL RESERVE**
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.