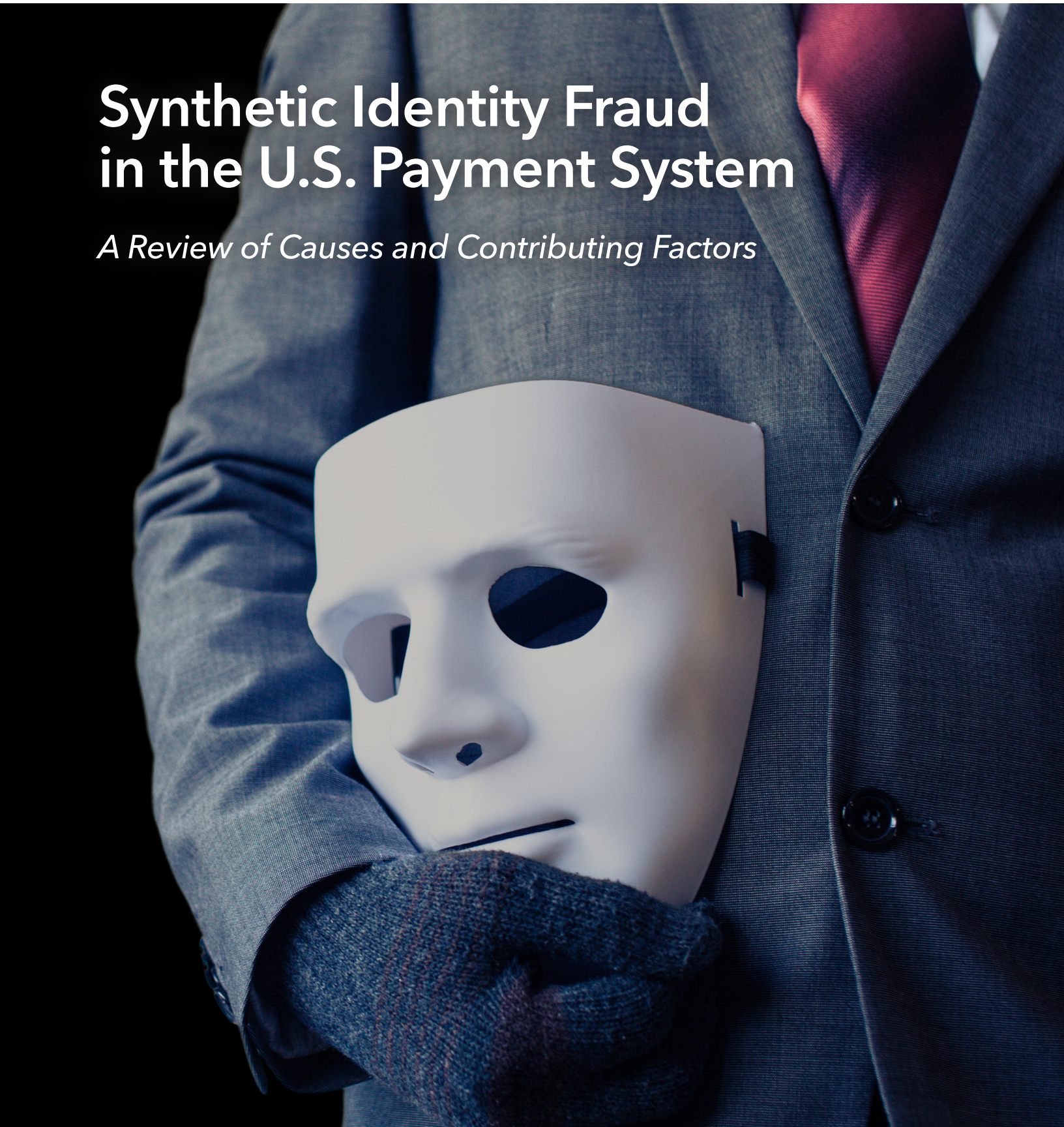
THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

PAYMENTS FRAUD INSIGHTS
JULY 2019

Synthetic Identity Fraud in the U.S. Payment System

A Review of Causes and Contributing Factors



FOREWORD

Table of Contents

The U.S. payment system faces dynamic, persistent and rapidly escalating threats as technological developments in cybercrime make it easier than ever to commit payments fraud. Since 2015, the Federal Reserve has collaborated with a wide array of industry stakeholders to advance U.S. payments security. This is consistent with the approaches described in our paper, *Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey*.

Late in 2018, the Federal Reserve launched an initiative to raise awareness and encourage action on the growing problem of synthetic identity payments fraud in the United States. Through primary and secondary research and industry dialogue, we seek to improve understanding of the issue, create a greater sense of urgency about addressing it, and promote industry action to both identify and mitigate this type of fraud.

This white paper on synthetic identity payments fraud is a compilation of insights from Federal Reserve and industry subject matter experts. It's intended to be a resource for industry professionals on the current state of synthetic identity fraud, including the scope of the issue, causes, contributing factors and its impact on the payments industry. Subsequent installments in our *Payments Fraud Insights* series will describe potential gaps in detection and mitigation approaches, as well as ideas and best practices to address the issue.

We would like to acknowledge and thank all the subject matter experts whose knowledge and insights contributed to the findings of this white paper. We look forward to continued dialogue with you, and with others in the industry, as we conduct additional research this year on synthetic identity payments fraud.

Ken Montgomery
Payments Security Strategy Leader, Federal Reserve System
First Vice President and Chief Operating Officer,
Federal Reserve Bank of Boston

THE FASTEST-GROWING TYPE OF FINANCIAL CRIME IN THE UNITED STATES

Synthetic identities can be used to deceive government or corporate systems into thinking they are real people – creating far-reaching impacts on the U.S. financial system, healthcare industry, government entities and individual consumers. While synthetic identities are sometimes used without criminal intent, there are serious consequences when criminals use them to steal funds, escape detection or facilitate drug and human trafficking. They also have been linked to crime rings, including those that fund terrorism.

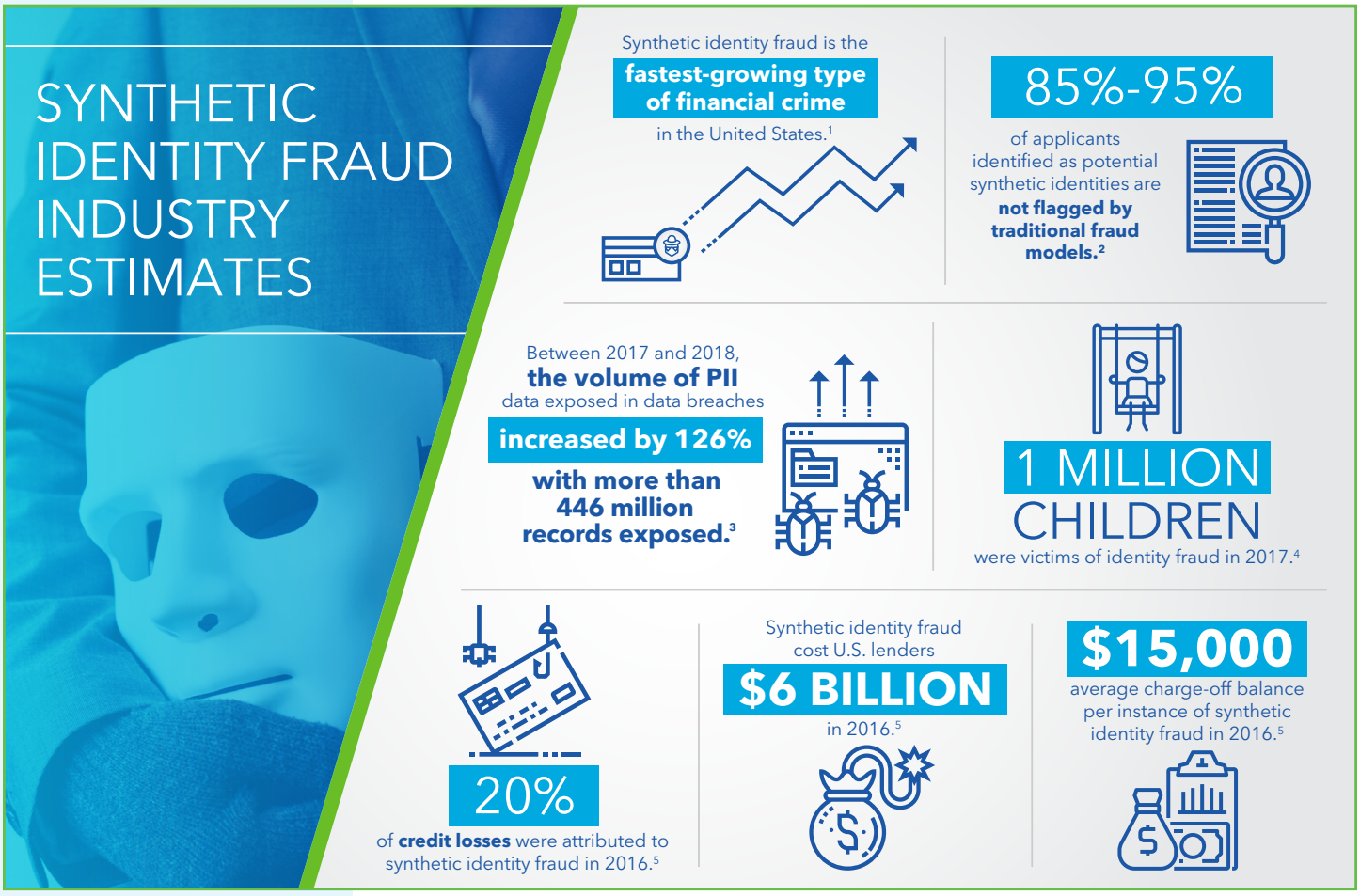
Synthetic identities tend to be more prevalent in the United States than in other countries because identification in the United States relies heavily on static personally identifiable information (PII), including Social Security numbers (SSNs). Although it is considered to be a new type of fraud, synthetic identity fraud existed for years in the United States before the widespread use of computers and the internet. In the past, this type of fraud was usually a face-to-face crime. Fraudsters were not only motivated by money, but in some cases, assumed a new identity if they were in trouble, in debt or wanted to make a fresh start. As the internet grew and digitization of financial systems took hold, fraudsters honed their technical skills and defined new methods to capitalize on synthetic identities to commit fraud.

Victims of synthetic identity fraud are typically children, the elderly or the homeless.

McKinsey estimates that synthetic identity fraud is the fastest-growing type of financial crime in the United States. However, synthetic identity fraud is difficult to detect. It is often unreported, since victims are typically individuals – such as children, the elderly or homeless – who are less likely to access their credit information

and uncover the fraud. This, combined with gaps in the credit process and the potential for large payouts, has made synthetic identity fraud attractive to criminals and crime rings.

Industry experts agree that synthetic identity payments fraud is difficult to measure due to inconsistencies in definitions and detection approaches. The figures throughout this paper are estimates that illustrate the potential magnitude of synthetic identity fraud in the United States overall and, specifically, in the payments industry.



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*

WHAT IS SYNTHETIC IDENTITY PAYMENTS FRAUD?

The generally agreed-upon definition of synthetic identity fraud is a crime in which perpetrators combine fictitious and sometimes real information, such as SSNs and names, to create new identities to defraud financial institutions, government agencies or individuals. However, industry experts tend to disagree on the classification of synthetic identity fraud and related mitigation approaches. Through ongoing analysis and by facilitating industry feedback, the Federal Reserve plans to work with the industry to determine how the classification of synthetic identity fraud best aligns with other fraud categories in the U.S. payments ecosystem.

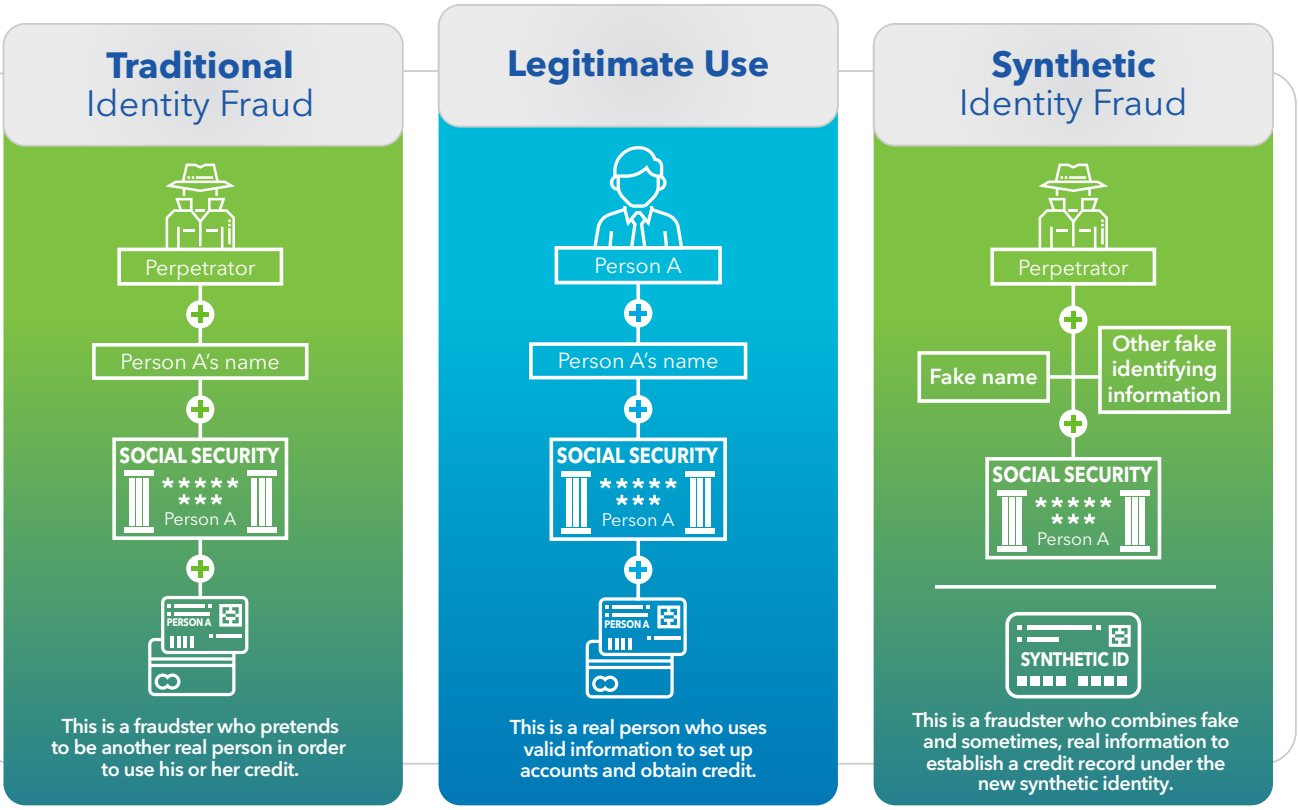
If you talk with numerous subject matter experts, you will hear almost equally numerous definitions of synthetic identity fraud.

How Synthetic Identity Fraud Differs from Traditional Identity Fraud

For the purpose of this paper, *traditional identity payments fraud* describes when a fraudster pretends to be another real person and uses his or her credit. The victim is directly affected financially, so this type of fraud is typically detected and reported relatively quickly.

In comparison, *synthetic identity payments fraud* is when a fraudster creates a new identity to commit fraud in one of several ways. Methods include *identity fabrication* (a completely fictitious identity without any real PII), *identity manipulation* (using slightly modified real PII to create a new identity), or *identity compilation* (a combination of real and fake PII, such as a false driver's license, to form a new identity).

DIFFERENTIATING TRADITIONAL IDENTITY FRAUD FROM SYNTHETIC IDENTITY FRAUD



It is often difficult to differentiate synthetic identity payments fraud from traditional identity payments fraud and legitimate financial activities. As a result, subject matter experts indicate that the number and volume of synthetic identities in financial portfolios are underestimated. For example, ID Analytics estimates that 85 percent to 95 percent of applicants who were identified as synthetic identities were not flagged as high risk by traditional fraud models, such as those used to detect traditional identity theft.

CAUSES AND CONTRIBUTING FACTORS

Fraud experts point out a number of reasons that criminals increasingly turn to synthetic identity payments fraud. Factors contributing to synthetic identity payments fraud include the near-universal use of SSNs as identifiers in the United States, data breaches that increasingly expose more PII, and gaps in the credit process. Together, these factors ensure that this type of fraud takes longer to detect and address.

Use of SSNs as Universally Used Identifiers

In 1936, the Social Security Administration (SSA) created SSNs for each individual solely to track earnings history, Social Security benefit entitlements and benefit levels. This unique identifier generally does not change over the individual's lifetime. As a result, the SSN has become an identifier that is universally used by private industry and other government agencies for a myriad of purposes.

In the past, SSNs were incorporated as identifiers into individuals' records and sometimes printed on driver's licenses, auto registrations, school IDs and Medicare cards. The value of stolen SSNs became more widely recognized as the internet matured and data breaches made PII more widely available. Today, even as SSNs are no longer widely used as identifiers on driver's licenses and other public documents, fraudsters continue to use SSNs as a key piece of information to create synthetic identities.

On June 25, 2011, the SSA began to randomly assign SSNs. According to the SSA, randomization was implemented to protect the integrity of SSNs and to extend the pool of nine-digit SSNs available nationwide. Randomization eliminated the geographical significance

of the first three digits of the SSN (also called the area number), which previously helped financial institutions determine an individual's state of origin. As a result of randomization, geographic checks are no longer effective for newly issued SSNs and it is more difficult to detect when fraudsters create synthetic identities using unissued or fabricated SSNs. ID Analytics estimates that nearly 40 percent of synthetic identities use a randomized SSN.

ID Analytics estimates that nearly 40 percent of synthetic identities use a randomized SSN.

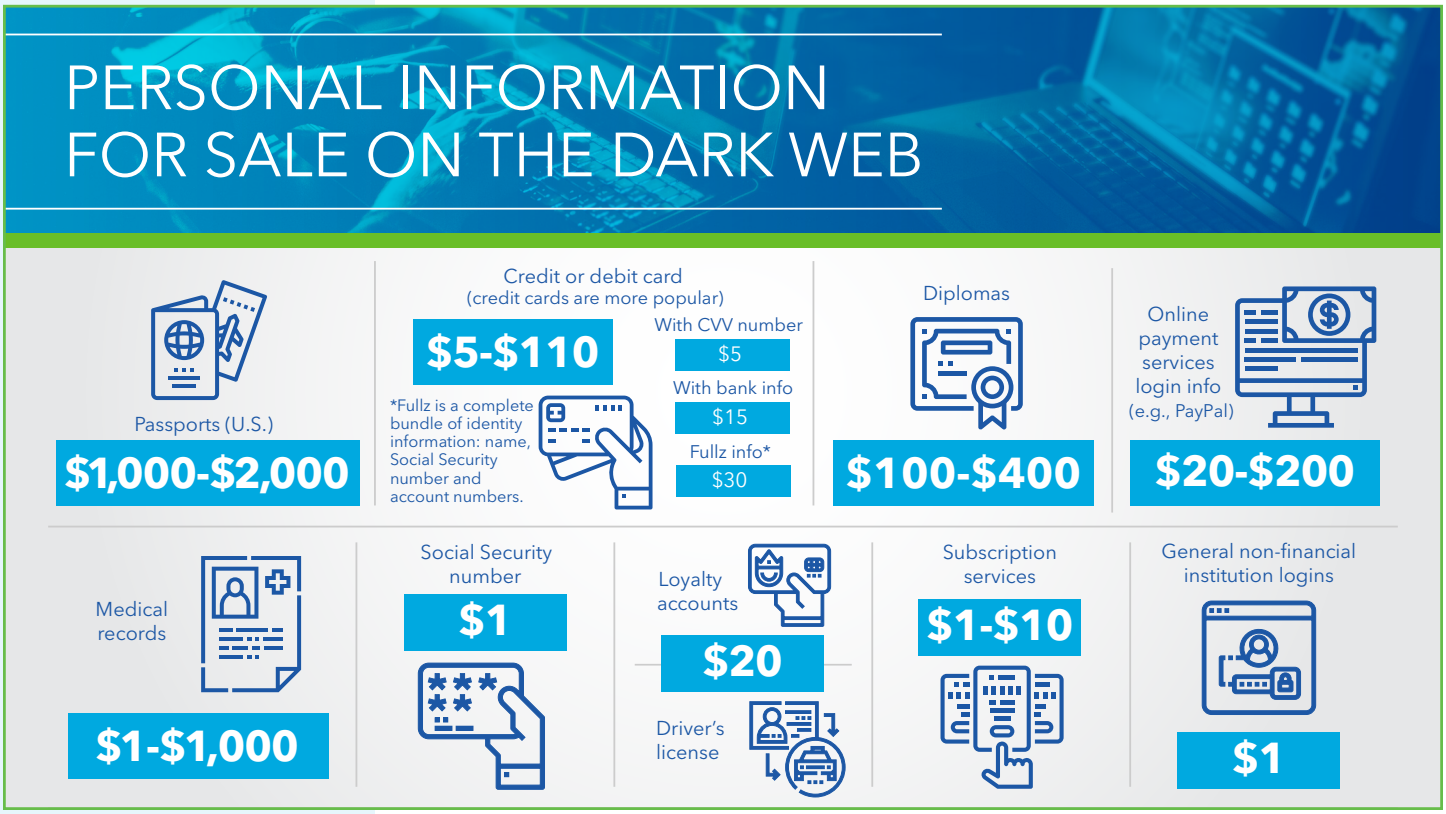
Instead of SSNs, fraudsters sometimes use nine-digit Credit Privacy Numbers (CPNs) to apply for credit and establish new credit profiles. CPNs are sometimes sold by non-reputable credit repair agencies to consumers who need to re-establish their credit. In reality, these CPNs may be valid but unissued SSNs, which are SSNs not yet assigned by the SSA. The use of CPNs to obtain credit is considered illegal by law enforcement officials, whether there is criminal intent or not.

To help control fraud, the SSA introduced a written Consent Based Social Security Number Verification (CBSV) service in 2008. This enables paid subscribers to verify a SSN holder's name and date of birth with written confirmation from the SSN holder. This paper-based verification process will be enhanced by an electronic version in the future, as a result of Section 215 of the Economic Growth, Regulatory Relief and Consumer Protection Act, which passed in 2018. Planning efforts for electronic verification are under way, with a pilot service expected to roll out in June 2020.

Increase in PII Available to Fraudsters

According to the Identity Theft Resource Center, the number of exposed PII records increased by 126 percent between 2017 and 2018, with more than 446 million records exposed due to data breaches. Combined with social engineering, personal information shared on social media and other risky behavior, this has increased the volume of PII available to build synthetic identities. The "dark web" – a subset of the internet inaccessible by traditional browsers and

search engines, and where content and activities are anonymous – offers large amounts of this information for sale, including bank account login credentials, driver's licenses, credit card numbers and SSNs.



Source: Experian (2019). *Here's How Much Your Personal Information is Selling for on the Dark Web*

Gaps in the Credit Process

Industry experts note gaps in the credit process that allow fraudsters to establish synthetic identities. For example, a fraudster applies for credit at a financial institution using a synthetic identity. Even if the financial institution rejects the credit application, the credit bureau automatically creates a new credit profile, since the applicant is considered new. The new credit profile becomes the synthetic identity's so-called "proof" of existence. The fraudster applies at a number of different financial institutions until an application is eventually approved. The credit bureau assumes the first applicant using a given SSN is legitimate. Any other individual who applies for credit using the same SSN then has to prove his or her identity – including the actual person whose SSN was stolen. Once the fraudster establishes a credit account with the synthetic identity, the goal is to quickly increase the identity's credit availability by cultivating a high credit score and then cashing out with the biggest payout possible.

HOW SYNTHETIC IDENTITIES ARE CREATED FOR USE IN PAYMENTS FRAUD

Step 1: Fraudster Creates an Identity Using Stolen or Fabricated PII

For many fraudsters, the process of creating a synthetic identity begins on the dark web, where they can purchase PII and other personal information exposed via various methods, including data breaches, social engineering, or oversharing on social media. Alternatively, fraudsters often fabricate all the information they use to apply for credit. If a valid SSN is used, it is typically one that belongs to a child or an elderly or homeless person who does not actively use or check his or her credit.

Step 2: Fraudster Applies for Credit Using the Synthetic Identity

ID Analytics estimates that more than 50 percent of fraudsters applied for credit online. Industry experts say that some fraudsters using synthetic identities also will show up in person at financial institutions, presenting false information to "prove" their identities. Once the fraudster applies for credit, the financial institution submits an inquiry to one or more credit bureaus, which will report that the identity does not have a credit history. As a result, the financial institution typically rejects this initial application for credit. However, this initial inquiry creates a credit file for the synthetic identity – even though the application was rejected.

Step 3: Fraudster Repeatedly Applies for Credit Until Approved

The fraudster continues to apply for credit at various financial institutions until one finally grants approval. In some cases, this initial approval is granted by a high-risk lender. The fraudster will use this line of credit and establish a timely repayment history to cultivate higher credit limits and additional accounts. This cultivation can take place over months or even years, especially when the owners of these SSNs are not active in the credit system.

Step 4: Fraudster Accelerates a Positive Credit History

The fraudster can accelerate the process of building good credit by piggybacking – being added as an authorized user to an account with good credit in return for compensation to that existing account holder. Piggybacking also can occur on another established synthetic identity with a positive credit history, or on synthetic identities associated with fictitious businesses, which also may extend lines of credit. ID Analytics estimates that nearly 50 percent of synthetic identities use piggybacking to build credit.

Fraudsters employ a variety of tactics to make the synthetic identity appear to be real and ensure high payouts. These include creating false identification documents, establishing a social media presence, and using drop addresses (e.g., P.O. Box addresses or addresses of vacant properties or vacation homes) that allow fraudsters to receive or forward credit cards or goods to alternate locations. Fraudsters also use synthetic identities to create fake businesses and sign up with merchant processors to obtain credit card terminals and run up charges on fraudulent cards. Sophisticated crime rings use these tactics at scale, developing intricate networks that support the cultivation of synthetic identities to commit fraud.

Step 5: Fraudster Busts Out

As a synthetic identity's credit score rises, the fraudster can secure larger extensions of credit until ultimately, the fraudster "busts out." This term refers to maxing out the credit line and vanishing. In addition, it is possible for a fraudster to double the payout on each credit line by claiming identity theft to have charges removed or by using fake checks to pay off balances before maxing out the credit again and defaulting. The fraudsters then can create new synthetic identities and repeat the process.

A COMPLEX INTERNATIONAL CRIME RING CASHES IN

In 2013, the Department of Justice charged 18 people as co-conspirators in "one of the biggest, most complex credit card fraud schemes ever." Over 10 years, a crime ring spanning 28 states and eight countries developed a network of more than 7,000 synthetic identities to fraudulently obtain more than 25,000 credit cards. The conspirators built up the synthetic identities' credit scores to increase their spending and borrowing power, and then maxed out these accounts without repaying.

The crime ring set up more than 7,000 synthetic identities to fraudulently obtain more than 25,000 credit cards.

The fraudsters created the synthetic identities by combining unissued SSNs with fake personal information. They maintained 1,800 drop addresses to use as mailing addresses. They obtained thousands of credit cards with low spending limits and increased spending power over time by making a series of small purchases and regular payments. The ring also boosted credit limits through piggybacking schemes, including placing classified ads offering compensation to unwitting consumers for adding the synthetic IDs as authorized purchasers on their accounts.

The crime ring set up 80 sham companies with little or no legitimate business. These sham companies established accounts with merchant processors to acquire credit card terminals and ran up charges on the fraudulent credit cards, even though no merchandise was exchanged. The merchant processors received the payments from the credit card companies and deposited the amounts into the business

accounts, which were withdrawn or wired overseas. Fraudsters also forged relationships with complicit businesses to run credit cards on their terminals and split the profits. As fraud was detected and merchant processors shut down accounts, the ring created new sham businesses, acquired new terminals and repeated the process.

By the time the fraud ring was uncovered, more than $200 million had been stolen.

The crime ring also used these sham companies to establish lines of credit for the synthetic identities. The companies provided payment information to credit bureaus to boost credit scores, reported false account payoff activity and backdated account openings to create the appearance of longstanding customers.

The crime ring generated huge profits. Its members spent lavishly on luxury goods, cars, electronics and gold. They stockpiled large sums of cash and wired millions of dollars overseas to a global network of co-conspirators. By the time the fraud ring was uncovered, more than $200 million had been stolen. Some industry experts speculate that the actual loss was close to $1 billion, but the true number is difficult to determine due to the complexity and longstanding nature of the fraud.

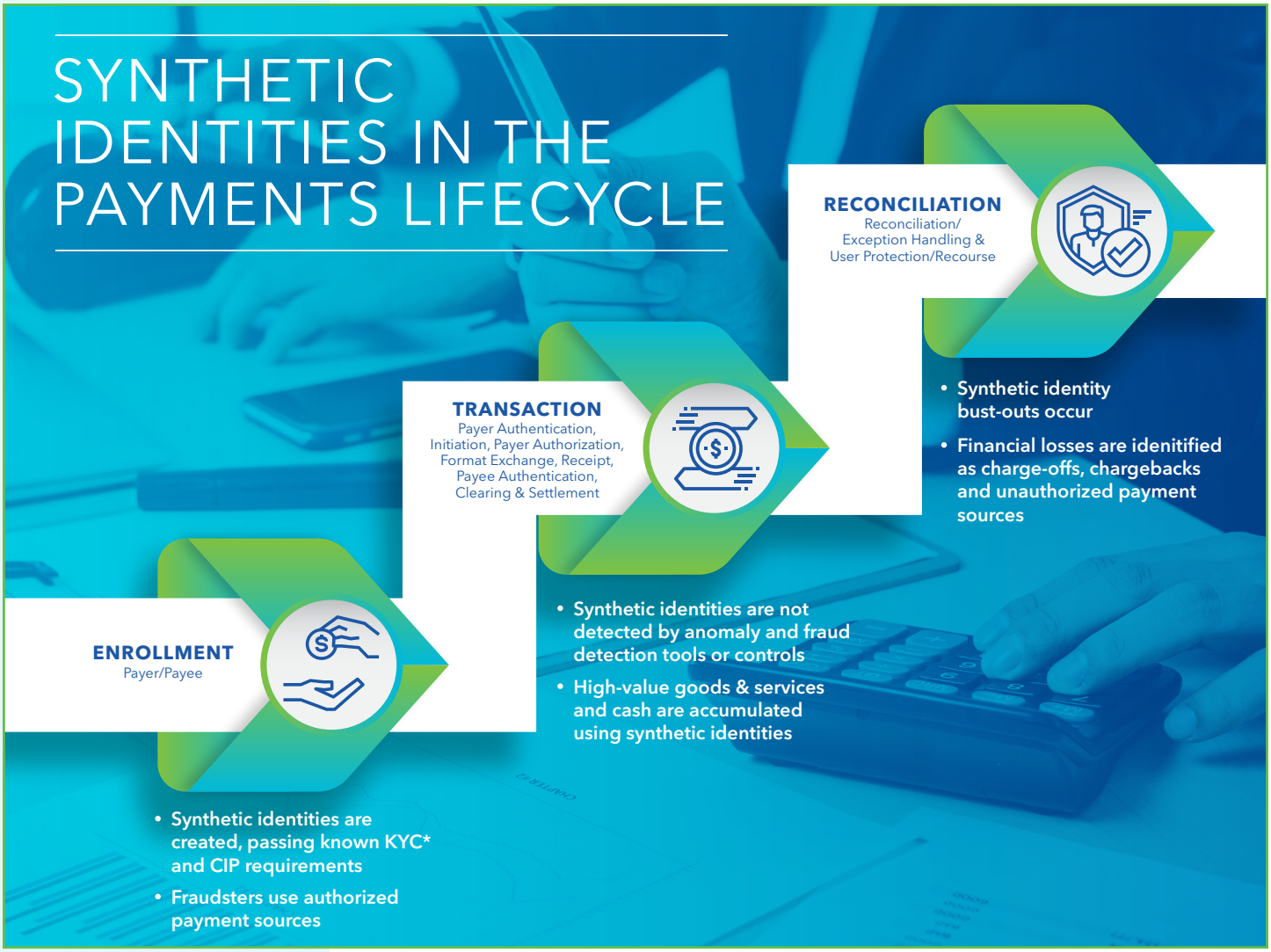
The case is now closed. Most of the defendants pleaded guilty to charges that included bank fraud, conspiracy to commit bank fraud, wire fraud and access device fraud. While most defendants served time, the Office of the U.S. Attorneys dismissed indictments in a few instances.

WHO BEARS THE COSTS?

In general, individuals whose SSNs are being used by synthetic identities are not responsible for the financial cost of the crime (excluding out-of-pocket costs) – as long as they can prove they are not behind the synthetic identities. Instead, financial institutions bear the majority of the cost of this type of fraud. Auriemma Group estimates that lenders in the United States incurred $6 billion in synthetic identity fraud costs in 2016. This estimate does not include monetary losses incurred by non-financial institutions, including merchant losses resulting from the issuance of store cards or auto lenders. Auriemma Group further estimates that the average charge-off balance per instance of synthetic identity fraud averaged more than $15,000 per attack, accounting for up to 20 percent of all credit losses in 2016.

Synthetic identities are found in all phases of the payments lifecycle.

The main goal of any payment system is to transfer funds securely from payer to payee. The overall process can be illustrated by the three phases in the payments lifecycle: enrollment, transaction processing and reconciliation. Synthetic identity fraud impacts each of these areas in different ways.



* KYC (Know your Customer) and CIP (Customer Identification Program) requirements were established as part of the Bank Secrecy Act, which requires businesses to verify identities before opening accounts. For more information on payments lifecycles, visit www.securepaymentstaskforce.org/learn-how-payments-work.

In the **enrollment phase**, fraudsters register previously created synthetic identities to apply for credit. These identities often pass Know Your Customer (KYC) requirements. Synthetic identity fraud in the enrollment phase poses reputational risk to institutions, as well as the risk of fines for KYC noncompliance. Additional costs can include operational costs (account set-up, maintenance, card activation and enrollment) incurred by the financial institution for processing and enrollment of new synthetic identity accounts.

The **transaction phase** – where the fraudster uses his or her synthetic identity to accumulate high-value and highly liquid goods and services, including electronic devices, gold or cash advances – poses the largest financial risk to financial institutions. In this phase, fraudsters also may create fake businesses to increase profitability

and the volume of transactions. Once fraudsters accrue a lucrative-enough gain, they bust out and cease payments on the account. In addition, they may fund payments with stolen bank accounts or claim identity theft. Financial institutions experience the monetary loss because they assume financial responsibility for unpaid balances.

During the **reconciliation phase**, financial losses due to synthetic identity fraud are typically identified as either charge-offs, chargebacks or unauthorized payment sources. Once accounts reach delinquency, each financial institution reports the losses based on their individual risk management policies. Some may report it as a credit loss, while others report it as a fraud loss. If the bad debt can be sold to a collection agency, a percentage of the monetary losses may be recouped by the sale. However, losses can increase due to collection costs, such as for demand notices and additional employee pay.

The true cost of synthetic identity fraud in the payments industry is difficult to quantify due to factors that include:

- ***Lack of consistency in identifying synthetic identities.*** Industry experts vary in their assessments of characteristics that differentiate synthetic identity fraud from either traditional identity fraud or legitimate consumers.
- ***Lack of investigation.*** It can be difficult to identify whether a charge-off, chargeback or unauthorized payment is the result of fraud or a credit loss. Once an account defaults, financial institutions may choose not to incur the cost of retrospective investigation of the delinquency causes.
- ***Lack of awareness.*** If synthetic identity payments fraud is not identified as a risk, losses caused by this type of fraud may not be resolved and could be written off.
- ***Lack of reporting.*** Operational costs for detection and mitigation often are not reported.

CONSUMER HEADACHES: STRAIGHTENING OUT THEIR RECORDS

The consequences of synthetic identity fraud on consumers, particularly vulnerable populations (e.g., children, the homeless, the elderly), may not be identified until years after their PII was compromised. According to the Child Identity Fraud Study conducted by Javelin Strategy & Research, more than a million children were victims of identity fraud in 2017. While this figure is not specific to synthetic identity payments fraud, it indicates the potential magnitude of risk to children, who are a favorite target for this type of fraud. Synthetic identity fraud can lie dormant for years, only being uncovered once individuals turn 18 and apply for their first car or student loans. Other consequences of synthetic identity fraud extend beyond payments fraud to include denial of disability benefits, rejection of tax returns and inaccuracies in health records.

Synthetic identity fraud can lie dormant for years, only being uncovered once individuals turn 18 and apply for their first car or student loans.

For consumers whose SSNs have been compromised, the process of reclaiming their SSNs can be time-consuming – particularly in cases where the fraudster established a credit file over a period of years or charged off a large amount of debt. Credit bureaus and financial institutions generally presume that the first individual to establish credit under a given SSN is the valid SSN holder. As a result, the real individual whose SSN has been used in synthetic identity fraud will be faced with the arduous task of proving his or her identity and taking steps to clean up his or her credit report. Although financial liability may be limited, legal fees are among the out-of-pocket expenses that can be incurred. The Federal Trade Commission is one of the organizations that provides information and assistance to consumers who are victims of synthetic identity fraud.

CONCLUSION

Synthetic identity fraud is a growing problem in the U.S. payments ecosystem that affects consumers, small and large businesses, financial institutions, government agencies and the healthcare industry. Fraudsters are more sophisticated and organized, crime rings are run as lucrative businesses, data breaches are frequent and the availability of PII on the dark web is staggering. We expect fraudsters will continue to commit this type of crime due to the lack of victims reporting fraud, difficulty in detection and high payoffs for fraudsters – compounded by increased digitization of the financial system.

Like cybercrime, the growing problem of synthetic identity payments fraud cannot be addressed by any government or private sector organization working in isolation. It requires the attention of all payments industry stakeholders to collaborate and work together to understand, detect, mitigate and address synthetic identity fraud in the U.S. payments ecosystem. The Federal Reserve will continue to work transparently and collaboratively with the industry to address the issue of synthetic identity payments fraud, with near-term plans to explore and document the current state of synthetic identity detection, controls and gaps.

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.