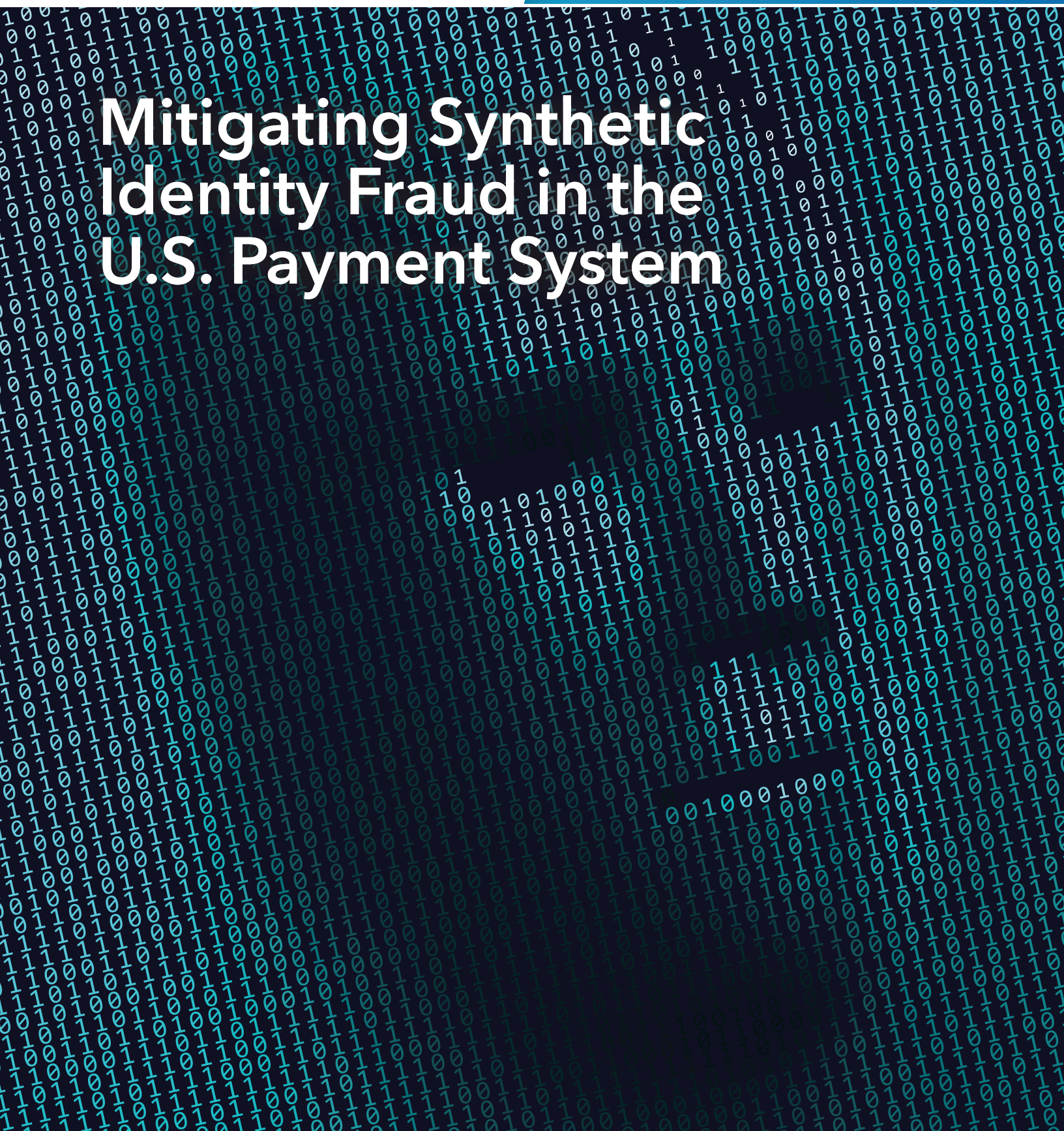
THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

PAYMENTS FRAUD INSIGHTS
JULY 2020

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



FOREWORD

Table of Contents

In 2019, the Federal Reserve published two white papers as part of our *Payments Fraud Insights* series. Our goal was to raise awareness and encourage industry action against synthetic identity fraud, reportedly the fastest-growing type of financial crime facing the United States. The first paper focused on causes and contributing factors of synthetic identity fraud and its impact on the U.S. payment system, while the second focused on detecting synthetics and examples of sharing information across the industry.

This white paper picks up where our last one left off. It highlights different ways that organizations – both individually and collectively – can work to mitigate synthetic identity fraud. Additionally, we summarize a number of external factors that impact mitigation, such as the regulatory environment.

Synthetic identity fraud is not a problem that any one organization or industry can tackle independently, given its far-reaching effects on the U.S. financial system, private industries – such as healthcare, automotive and insurance – government entities and consumers. The Federal Reserve recognizes the need for collaboration as we work with a wide array of payments industry stakeholders to advance U.S. payments security, which 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*. Our *Payments Fraud Insights* white papers were made possible by the contributions of many industry and government subject matter experts and Federal Reserve colleagues. We appreciate your shared insights and look forward to continued dialogue and collaboration in reducing synthetic identity payments fraud.

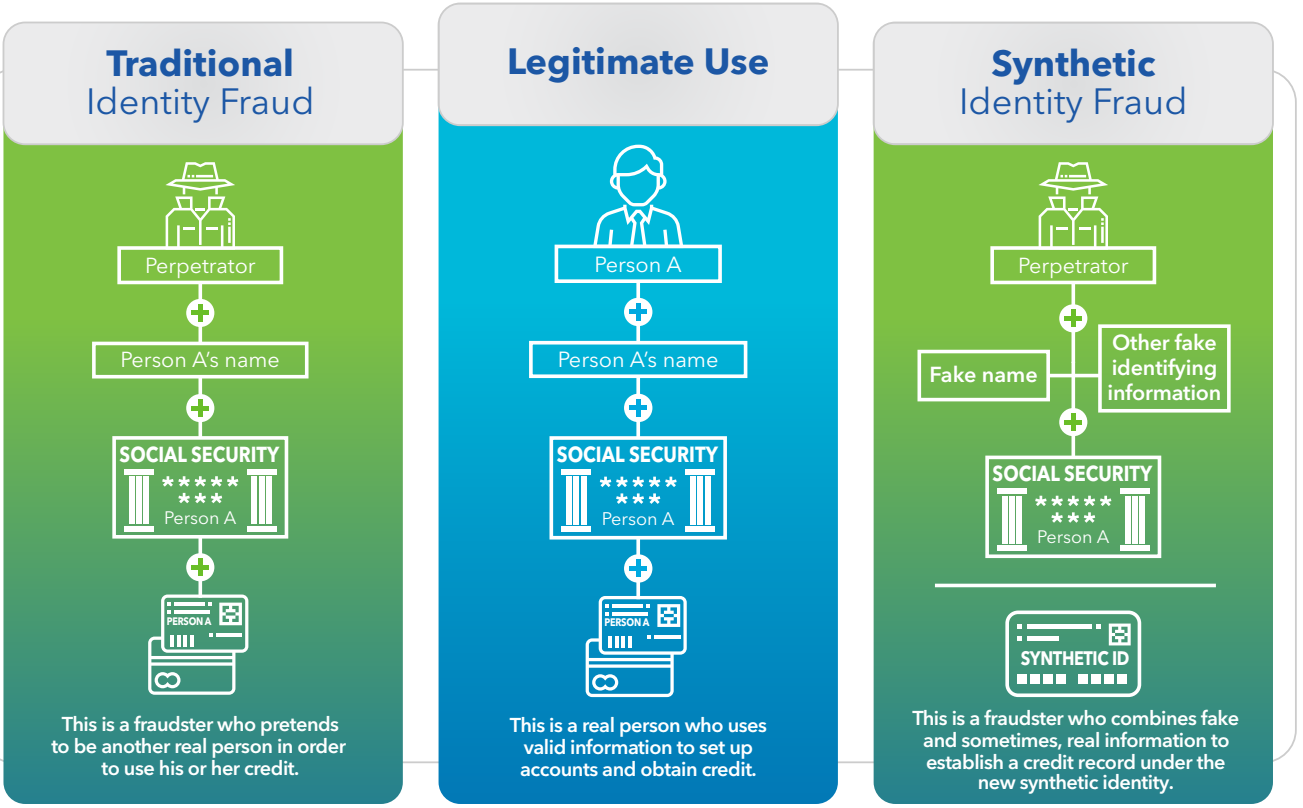
Jim Cunha
Payments Security Strategy Leader and Fintech Division Head
Senior Vice President, Federal Reserve Bank of Boston

KEY FINDINGS: FEDERAL RESERVE 2019 WHITE PAPERS

Synthetic identity fraud occurs when perpetrators combine fictitious and sometimes, real information, such as names and Social Security numbers (SSNs), to create new identities. These identities may then be used to defraud financial institutions, private industry, government agencies or individuals. Differing definitions and approaches to detection make it difficult to quantify the impact on the U.S. financial system. One widely reported analysis by Auriemma Group suggested that synthetic identity fraud cost U.S. lenders $6 billion and accounted for 20% of credit losses in 2016.

Our first white paper, *Synthetic Identity Fraud in the U.S. Payment System*, described key characteristics of this type of fraud. Fraudsters leverage the personally identifiable information (PII) of individuals – frequently 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 conventional 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" – the process of maxing out a line of credit with no intention to repay.

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 financial institutions, private industry, government agencies and individuals. 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 several contributing factors leading to an increase in 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, though they have evolved into a principal way that private industry and government agencies identify people and assess their legitimacy. The SSA also began randomizing the assignment of SSNs in 2011, eliminating the geographical significance of the first three digits (the area number) and thus, the predictable, chronological significance of the remaining digits.

- **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.

- **Credit process gaps.** The fraudster can leverage legitimate processes, such as 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. Fraudsters also can piggyback new synthetics onto accounts owned by established synthetic identities, or "sleepers," within a portfolio.

More than 446 million records were breached in 2018, representing a 126% increase from 2017.

The most likely point of detecting a synthetic identity is when a fraudster applies for credit. Fraudsters can leverage a variety of tactics to cultivate synthetics, including the fabrication of identification credentials, social media profiles and other documentation to make them appear legitimate. An ID Analytics study found that only half of synthetics apply for credit using digital channels, indicating a significant number of fraudsters are able to pass Know Your Customer (KYC) tests even when appearing in person.

In our second white paper, *Detecting Synthetic Identity Fraud in the U.S. Payment System*, we stressed the importance of looking beyond the basic required identifying information in order to verify whether an identity is legitimate or synthetic. Some characteristics of synthetic identities include:

- Credit file depth is inconsistent with customer age or other profile information
- Multiple identities with the same SSN
- Multiple applications from the same phone number, mailing address or IP address
- Use of secured credit lines or piggybacking to build credit
- SSN issued after 2011
- Multiple authorized users on the same account

However, focusing on any one characteristic alone could lead to false positives or disadvantage certain types of legitimate customers, such as recent immigrants with short credit histories. Rather, it is important to look across multiple characteristics and data sources to identify synthetics. For example, another source of data appears after a fraudster busts out. If the financial institution categorizes the loss associated with the bust-out as fraud, rather than as a credit loss, it can use the information to identify linked accounts (e.g., other accounts with the same SSN, name, address, etc.) or other associated identities.

No single organization can stop synthetic identity fraud on its own.

No single organization can stop 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, share information and keep up with the threat.

INTRODUCTION

Over the past year, we have spoken with more than 50 industry experts about synthetic identity payments fraud and its impact on the financial services industry. These experts represent a broad spectrum, spanning financial institutions, consulting firms, government agencies, industry organizations and consortia, service providers and technology companies. In our most recent discussions, we asked for their insights on current trends, detection and mitigation strategies, and where they expect fraud tactics to move in the future.

Coalesce estimated that synthetic identities account for slightly more than 20% of all losses in a given loan portfolio, even though they account for less than 1% of all loans.

Software company SentiLink reported finding synthetic identities in 0.3% to 0.6% of new accounts, but estimated that some financial institutions' rates of approved accounts that were issued to a synthetic identity could be as high as 2.7% of all new accounts. A study conducted by AI company Coalesce estimated that synthetic identities account for slightly more than 20% of all losses in a given loan portfolio, even though they account for less than 1% of all loans. Coalesce estimates that synthetic identity fraud losses average 4.6 times a typical credit loss. Both SentiLink and Coalesce estimates are based on data from smaller financial institutions and as a result, may not be representative of the industry overall. These statistics are important, however, as many small to mid-size financial institutions do not believe they are potential targets of this fraud threat.

In this paper, we discuss:

- How institutions approach synthetic identity fraud mitigation individually;
- How they can or do work collaboratively with industry partners; and
- How mitigation is influenced by the regulatory environment and other external factors.

Although this paper is focused on mitigating synthetic identities from the point of view of the U.S. financial services industry, we recognize that the impacts of synthetic identity fraud are far-reaching and touch many industries.

HOW ORGANIZATIONS CAN MITIGATE SYNTHETIC IDENTITY FRAUD

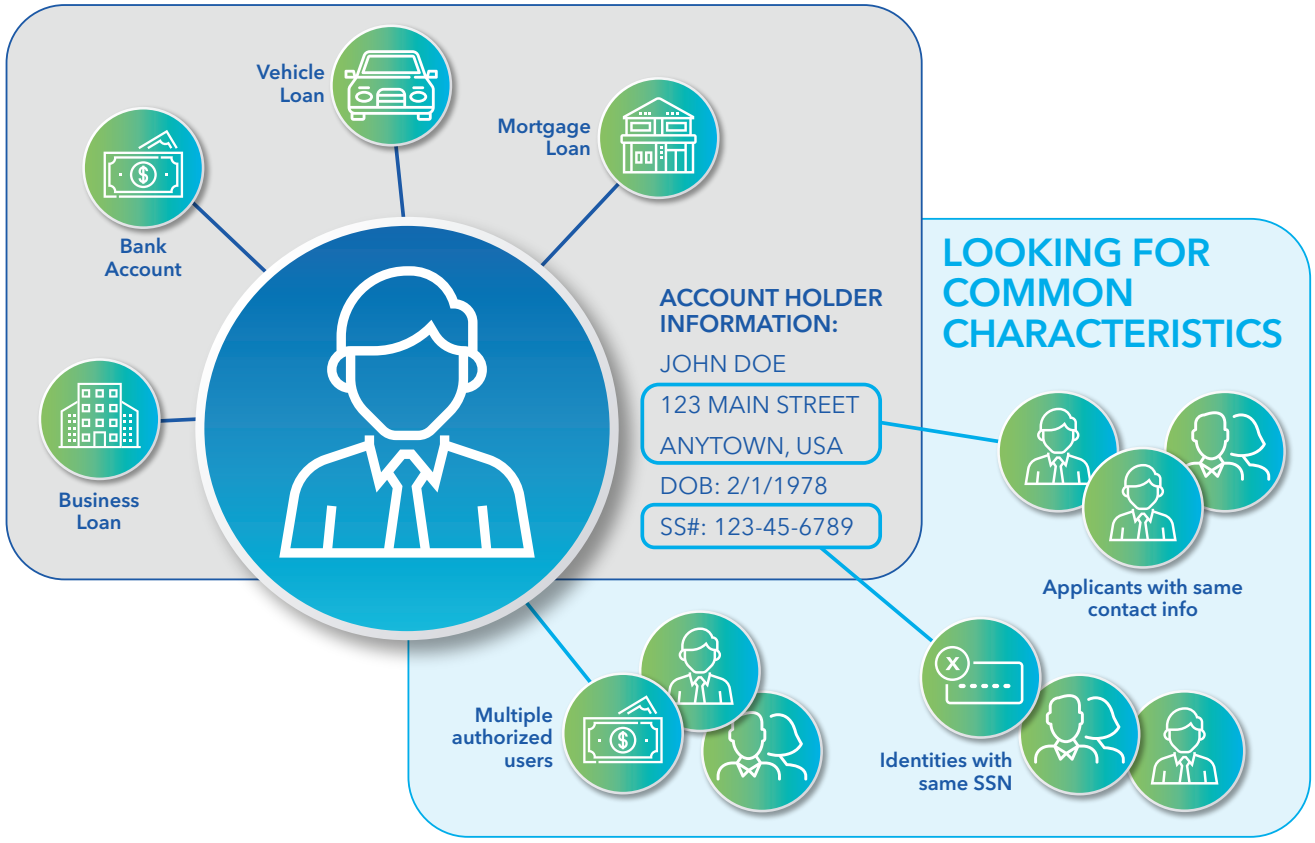
Industry experts recommend a comprehensive approach to mitigating synthetic identity fraud, noting that there is no one-size-fits-all solution to this growing problem. A multi-layered approach that employs both manual and technological data analysis gives organizations the best chance to identify and mitigate fraud caused by synthetics.

Synthetic identity accounts behave more like normal customers – building credit over a period of time – than conventional identity fraudsters, who must rapidly cash in before the victim notices and reports the theft. According to fraud industry experts, organizations that have the most success are those that look beyond basic PII elements (such as name, SSN, date of birth and address) and use additional data sources to gain reasonable assurance of the applicant's identity.

Experts also mentioned the benefits of robust link analysis processes – processes that look across various banking instruments (such as checking accounts, lending accounts and other financial instruments) to identify relationships or common characteristics of synthetic identities. Examples include identifying multiple users with the same SSN, screening for multiple account applications originating from the same IP address or device, and detecting potential fraud networks by linking identities that appear as authorized users on multiple accounts. Link analysis also can be conducted across multiple banks for service providers that have multiple financial institutions as clients.

We see increased use of artificial intelligence (AI) and machine learning – the use of technology to perform tasks that normally require human intelligence – to detect and mitigate synthetic identity fraud. AI and machine learning can create efficiencies for financial institutions, while also saving time and labor costs. We spoke with

LINK ANALYSIS CAN IDENTIFY OTHER SYNTHETIC IDENTITIES AND ACCOUNTS



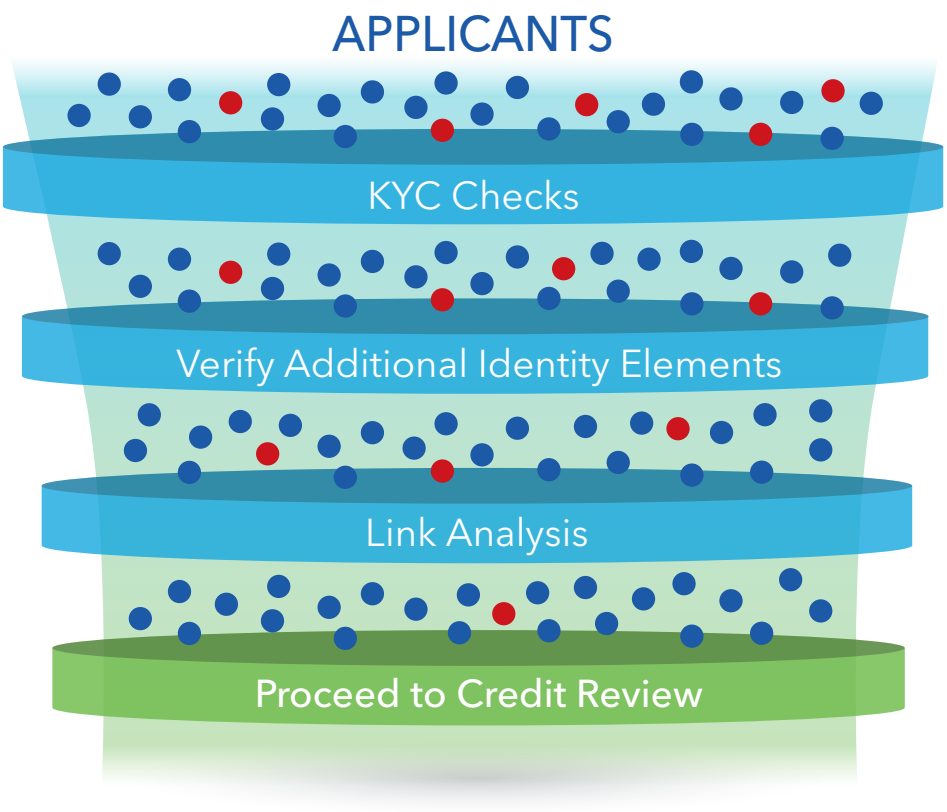
one credit union service organization that cited the value of integrating technology into fraud detection and analysis processes, as there is more data available than humans can possibly analyze manually. While AI provides many benefits, industry experts note that false positives in customer identity information can be difficult for consumers to rectify. One such example is a mismatch in consumer information due to name variations (such as a consumer using the name Bob instead of Robert). This can create additional customer friction for many organizations, and underscores the need to avoid reliance on any one approach.

Traditional fraud models are not designed to detect synthetic identities. An ID Analytics study estimated traditional fraud models were ineffective at catching 85% to 95% of likely synthetic identities. However, as technology has continued to develop, AI tools and models have continued to become increasingly more effective.

We recently spoke with a credit union about its machine learning tool developed for fraud detection. In beta tests, the tool flagged approximately 85% of credit applications originating from synthetic identities. While this demonstrates that detection models can successfully be adapted to synthetics, fraud industry experts advise that these detection models could be improved if they utilize a standard definition of synthetic identity fraud. This would allow for broader comparison and analysis of the data and results.

Subject matter experts also recommended that financial institutions work to break down their internal barriers to facilitate sharing of information across product lines. Synthetic identity fraudsters generally open multiple accounts at the same organization. If a synthetic identity has a credit card, it also may own a direct deposit account, line of credit, auto loan or mortgage, as well. If the identity busts out on one account, it's likely to bust out on other accounts around the same time – emphasizing the urgency to minimize losses by connecting these accounts quickly.

MULTI-LAYERED MITIGATION MUST BE BALANCED WITH THE CUSTOMER EXPERIENCE



THE IMPORTANCE OF WORKING TOGETHER

Beyond calling for basic awareness on the scope and scale of synthetic identity payments fraud, experts stress the importance of 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. Collaboration provides stakeholders with larger data sets of fraud and account information. One expert said, "Consortium data is better than organization-level data in detecting trends." Information sharing is particularly important for smaller financial institutions, which generate less data and may have fewer technological and fraud-fighting resources than larger companies. That said, experts were quick to add that information sharing is only as effective as the quality and integrity of the data itself.

Experts were quick to add that information sharing was only as effective as the quality and integrity of the data itself.

One service provider we interviewed analyzes customer account data across hundreds of financial institutions to identify linkages to known synthetic identity accounts. This approach can better enable fraud mitigation and prevent significant financial losses for institutions.

It is vitally important for law enforcement and financial institutions to share information about threats and trends, which in turn, supports effective investigations. Information sharing must comply with applicable laws and regulations. For example, Section 314(a) of the USA PATRIOT Act allows law enforcement agencies to request information from participating financial institutions for terrorism or money laundering investigations, while Section 314(b) of the act allows participating financial institutions to share customer information with one another in support of their own due diligence, compliance and reporting requirements. Section 314(b) also allows for sharing information that relates to specified unlawful activities – which could be inclusive of fraud. Industry experts note that some financial institutions are uncertain which information would qualify for 314(b) safe harbor. In turn, this affects the amount and type of information shared by financial institutions.

While fraud industry experts advised that concern about regulatory risk and requirements may be a potential obstacle to financial institutions sharing information, this is not the only consideration. Financial institutions also may be concerned about losing their competitive advantages, incurring reputational risk and complying with data privacy and security requirements. However, these same experts expressed hope that the benefits of broader information sharing across the industry will begin to outweigh these factors.

Similarly, the experts interviewed noted that data security, as well as liability and legal compliance concerns, could potentially be addressed by creating platforms and/or consortia to provide validation without collecting or sharing sensitive customer data. One illustrative example they noted was the use of a central repository that participants could query to obtain confirmation that a customer meets an age requirement, without collecting, storing and sharing that customer's actual PII. This type of information sharing and validation may require some regulatory or legislative changes. Conceptually, this simple example illustrates a potential opportunity to remove barriers while limiting data security and liability vulnerabilities.

REGULATORY AND ENVIRONMENTAL INFLUENCES ON MITIGATION

The impact of synthetic identity fraud on the financial system has helped influence a number of regulatory and legislative changes over the past decade in an effort to help mitigate this type of fraud. One upcoming regulatory change for 2020 is the launch of the SSA's Electronic Consent Based SSN Verification Service (eCBSV). However, regulatory updates alone are not enough to completely eradicate this type of fraud. Rather, they should be used in conjunction with other controls to create an effective, multi-layered approach to fraud mitigation.

Initial Rollout of the Electronic Consent Based SSN Verification Service

Perhaps the most significant legislative synthetic identity fraud prevention development is the June 2020 initial rollout of the Social Security Administration's electronic Consent Based SSN Verification service. The SSA introduced the original Consent Based Social Security Number Verification (CBSV) service in 2008. This service enables paid subscribers, upon written consent from the SSN holder, to verify that a name, SSN and date of birth combination matches (or does not match) the SSA's records. Section 215 of the Economic Growth, Regulatory Relief and Consumer Protection Act mandated that the SSA develop an electronic version of the CBSV for permitted entities. The fee-based eCBSV will work largely the same as the original service, but will allow individuals to provide consent electronically rather than with a "wet" signature. This new service will allow financial institutions to validate information in real time and reduce customer friction by allowing electronic consent.

Experts have expressed optimism that electronic verification will reduce the prevalence and impact of synthetics in the financial system by blocking new synthetic accounts. However, they noted this will not be a complete solution. The service will be available only to financial institutions or service providers, subsidiaries, affiliates, agents, subcontractors or assignees of financial institutions. This may shift fraudster tactics, including attempts to create synthetics at other types of organizations without access to the eCBSV service.

Experts also suggested that additional modifications could potentially further enhance eCBSV's effectiveness in combatting synthetic identity fraud, including:

- **User types.** Service access could be broadened to include industries outside of financial services that also are impacted by synthetic identity fraud – such as telecommunications companies, medical providers and insurers. Within the financial services industry, access could be broadened to include non-lending branches (e.g., brokerage subsidiaries).

  Feedback provided by the SSA noted that potentially expanding access to the service to currently non-permitted entities may have additional security and integrity risks. It also may increase the usage of SSNs for purposes beyond its original intent; the more SSNs that are used unnecessarily, the greater the risk for misuse and abuse.

- **Service hours.** While the SSA has not yet set eCBSV service hours, it expects to provide at least the same availability as for CBSV. If so, the eCBSV system will be unavailable for periods overnight on weekdays and longer periods of time overnight on weekends.

  It is important to note that it is not yet clear how planned service outages will affect overnight application processing for financial institutions. When we spoke with the SSA, they noted these outages are necessary to ensure that data matches the most current information in the SSA database.

- **Approved eCBSV uses.** Currently, the eCBSV service only allows for customer information validation for new accounts. Experts have suggested that if the eCBSV service were expanded to include validation of information on existing accounts, financial institutions could more easily identify synthetics in their existing portfolios. However, according to the SSA, this is not possible, as the Privacy Act prohibits federal agencies from disclosing information without prior consumer consent.

Industry experts expect other types of fraud to increase as account onboarding controls better detect synthetic identities with the help of eCBSV and other methods. The industry may see a shift toward conventional identity theft, when accounts are opened using an individual's real name, real SSN and real date of birth – but the fraudster's contact information (such as address and phone number). To mitigate this likely shift in fraud tactics, the industry should preemptively work to increase mitigation controls for this type of fraud.

eCBSV SERVICE CAPABILITIES

The eCBSV service **WILL** be able to

- Validate customer name, date of birth and SSN for financial institutions
- Reduce customer friction by allowing electronic consumer consent for financial institutions
- Provide validation for new account applications

The eCBSV service **WILL NOT** be able to

- Allow non-financial institutions to use the validation service
- Provide 24/7 validation service
- Allow financial services to validate existing account data
- Eliminate the risk of all false positives for a financial institution

Impacts of Regulatory Changes

In our previous white papers, we examined how regulatory changes, even though well-intentioned, can have unintended consequences. Noteworthy examples include the SSA's introduction of randomized SSNs in 2011 – which was intended to protect the integrity and improve the longevity of the SSN system. However, it also made subsequently issued SSNs harder to validate, as it eliminated the geographic significance of the first three-digit area code.

A more recent example is the 2017 Federal Trade Commission (FTC) rule change that simplified the dispute processes for identity theft victims by eliminating the need for a police report. This change simplifies and streamlines identity theft claims for consumers. However, it also allows fraudsters to more easily dispute their negative credit information. Experts note that disputing credit file information is one strategy fraudsters employ in order to bust out more than once on the same synthetic identity.

The Fair Credit Reporting Act, Section 605B, mandates that once a consumer disputes information directly with a credit reporting agency (CRA), the financial institution has four days to address the dispute. This process is intended to decrease the amount of time it takes consumers to resolve inaccuracies on their credit reports. While this process benefits consumers, fraudsters have taken advantage of the change by flooding CRAs with invalid disputes.

The CRAs relay the information to financial institutions that may or may not have the bandwidth to process a full investigation within the four-day timeframe to determine whether it is a valid loss. If the deadline is missed, the CRA must delete the negative information from the credit report. This practice is termed "credit washing," and sometimes allows a synthetic to bust out more than once using the same identity. For example, a fraudster busts out, then claims to be the victim of identity theft by disputing the derogatory trade line information with the credit reporting agencies.

The reduced time to conduct a full investigation makes it more likely that negative information will be removed from the credit file of the synthetic identity, and allows the fraudster to reuse this identity to bust out again.

In all the above cases, the changes made were well intentioned and reflected various important public policy objectives, such as consumer protection. However, fraudsters will take advantage of all opportunities. It is important for all participants to try to understand how the fraudsters will exploit new processes and develop strategies to mitigate them.

The Importance of Data Integrity

Sharing of information is only valuable when participants can trust the integrity of the data that is being shared. Skilled synthetic identity fraudsters can manipulate the system to introduce fictitious information that is perceived to be accurate. For example, the Fair Credit Reporting Act requires that when a credit inquiry is submitted to a credit reporting agency, the credit reporting agency must create a credit file – whether or not the customer's identity has been validated. The existence of a credit file can seem to imply "proof of life" and validation of the identity, but it does not. Since KYC compliance validates static customer information that can be falsified – such as name, date of birth, SSN and address – many financial institutions look at additional data points to authenticate their customers.

Financial institutions may review customer data and identity elements that extend beyond credit bureau data – such as examining the length of time a customer's email address has been active or matching ownership data for the provided phone number and address. Additionally, the institution can verify whether this combination of information makes logical sense. For instance, a 50-year-old customer who has an email address that was active for only six months, and no active accounts over five years old, should raise a red flag. These types of identity authentication red flags have enabled financial institutions to more effectively understand who their customers are, and in turn, identify potential synthetics.

The Better Identity Coalition's 2018 paper, *Better Identity in America: A Blueprint for Policymakers*, recommended triangulating data from multiple sources to validate individuals – for instance, examining data from both the SSA and state motor vehicle databases. This approach avoids reliance on PII from singular

sources and helps organizations create a more complete picture of their customers. Integrating dynamic data sources, such as past transaction behavior, can further help organizations validate an identity, while limiting the risk of a static dataset being compromised.

Data Privacy Laws at the State Level

Data privacy laws prohibit the disclosure or misuse of consumer information and exist for the purpose of consumer protection. Data privacy laws in the United States are generally enforced at the state level. As a high number of data breaches over the past several years has made consumer information increasingly more available, protecting this data becomes more important than ever. Considered to be the most comprehensive state mandated consumer data privacy law, the California Consumer Privacy Act (CCPA) went into effect on January 1, 2020 with the following consumer protections:

- The right for a consumer to confirm if an institution is collecting personal data about him or her, and the right to access that personal data;
- The right for consumers to request deletion of personal data; and
- The right for a consumer to opt out of the sale of his or her personal data to third parties, such as for targeted advertising.

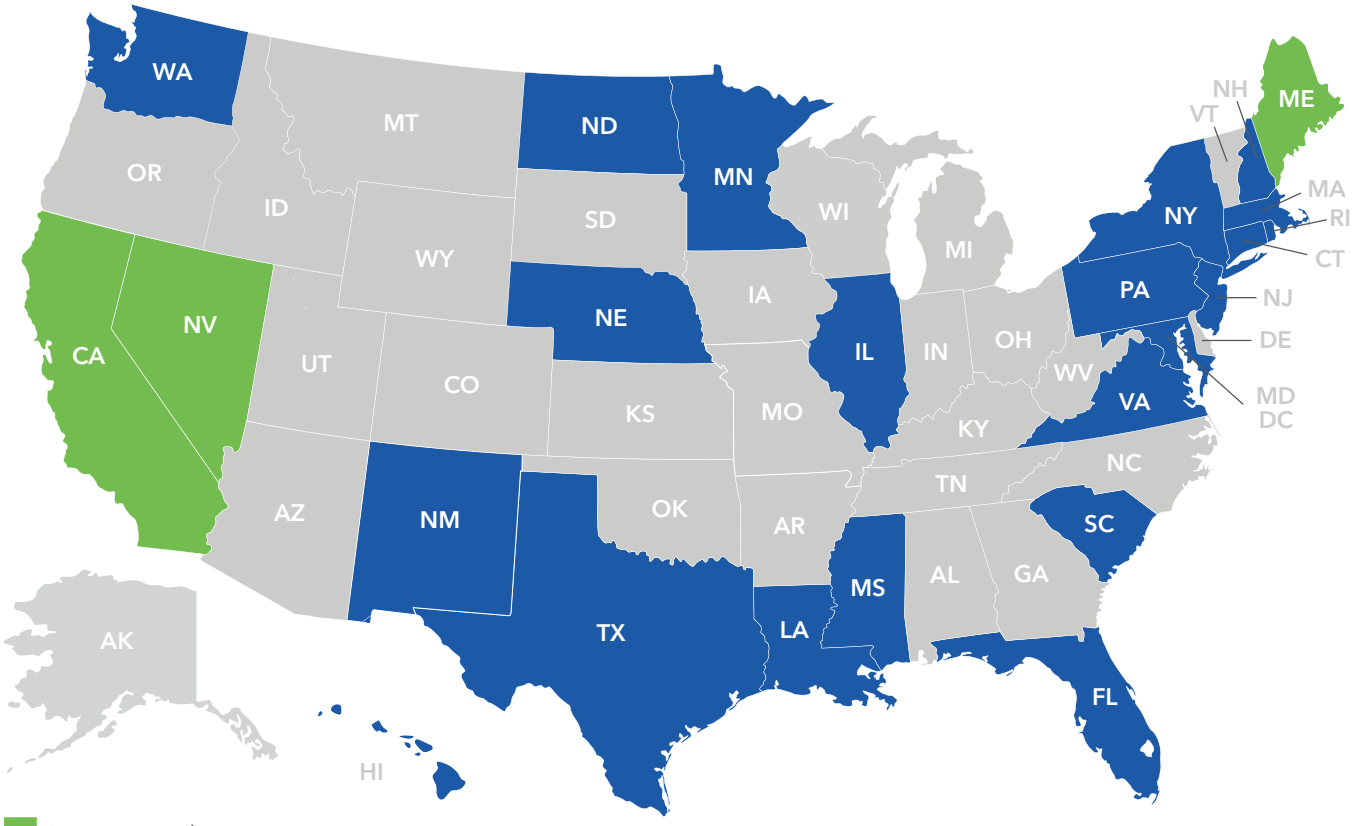
The adoption of CCPA has spurred other states to consider consumer data and privacy legislation, in an effort to further consumer protection. Currently, California, Nevada and Maine have legislation on consumer data privacy, and as of the publication date of this paper, six others have proposed legislation on consumer data privacy.

Experts note two potential unintended consequences of these consumer privacy and security laws:

- Fraudsters may leverage these laws to delete personal data about a synthetic identity.
- Financial institutions may become less willing to share information with others that could help mitigate synthetic identities.

Data protection and consumer privacy is increasingly in the public eye given the high number of data breaches over the past several years and increased availability of consumer data for sale on the dark web. Some experts have called for federal legislation for data protection and consumer privacy or other actions aimed at more consistency in these protections. One potential outcome of this would be to help prevent fraudsters from leveraging perceived gaps in legislation. The policy implications of such changes should be examined carefully to understand potential far-reaching effects.

STATE CONSUMER PRIVACY LAWS



Source: International Association of Privacy Professionals; information as of April 2020

CONCLUSION

There is no single solution to completely mitigate synthetic identity payments fraud. Factors such as the regulatory environment, technological advancement and shifts in fraudster tactics create a constantly evolving payments fraud landscape. Experts have suggested that a holistic approach would be the most effective way to mitigate synthetic identity fraud. This approach should include a consistent definition of synthetic identity fraud, technological innovation, robust data solutions for identity verification and an ongoing fraud mitigation dialogue between private industry and government agencies.

Information sharing within – and between – organizations also can help the industry draw connections between datasets to better identify potential synthetic identities. Technology can complement manual fraud mitigation practices, as AI and machine learning solutions help humans analyze this data more effectively than humans alone. While the technological capabilities of these models are developing rapidly, the industry must collect more and better data in order for these AI and machine learning solutions to improve their sensitivity and more successfully mitigate fraud.

The industry continues to make strides toward more effective mitigation solutions to reduce synthetic identity fraud. These include technological advancements, updated legislation intended to better protect consumers and services, such as the SSA's eCBSV. The Federal Reserve will continue to partner with industry stakeholders to raise awareness about synthetic identity fraud as we explore additional opportunities to actively collaborate with the industry to combat this type of fraud.

THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.