RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AFD-W01**

Connecting the Dots: Identifying and Mitigating Synthetic Identity Fraud

Mike Timoney

Vice President of Secure Payments,
Federal Reserve Bank of Boston

June 8, 2022

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

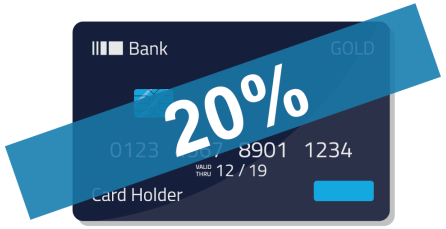
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

THE REAL PROBLEM OF A FAKE IDENTITY

Why Synthetic Identity Fraud is a Cause for Concern

Increase in cases

Losses growing year over year[1]



Losses often miscategorized[2]

Frequently targets vulnerable populations[3]

Sources: [1] ABA Banking Journal, [2] LexisNexis, [3] Carnegie Mellon CyLab

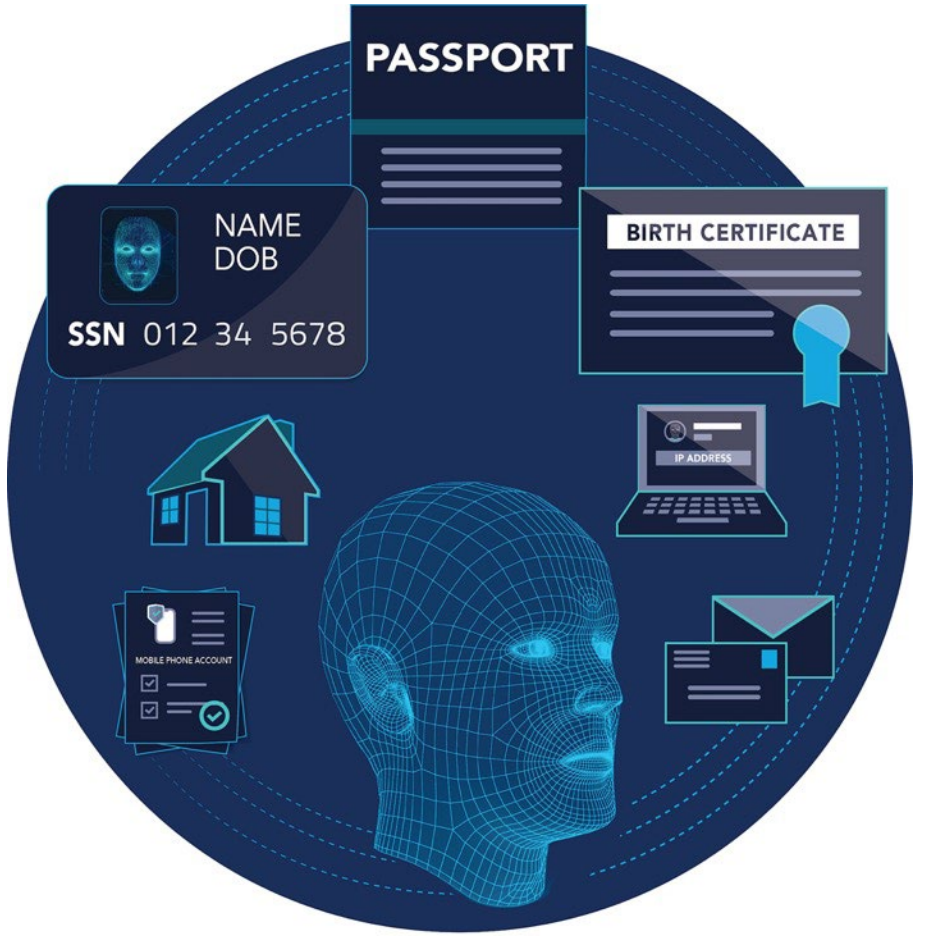
THE REAL PROBLEM OF A FAKE IDENTITY

What is Synthetic Identity Fraud?

- The use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain

- Different from conventional identity theft – implied identity not typically associated with a real person

The Federal Reserve led a focus group of industry experts to develop this industry-recommended definition to foster improved awareness, measurement, detection and mitigation.



THE REAL PROBLEM OF A FAKE IDENTITY

How Synthetic Identities are Typically Used to Commit Payments Fraud: Payment Default Scheme

Submits an application for credit

Results in creation of credit file

Repeatedly applies for credit until approved

Pays balances to increase creditworthiness

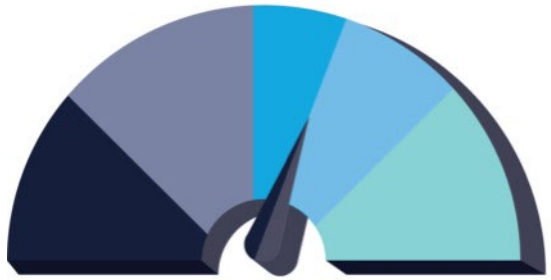
Busts out and disappears without repaying

THE REAL PROBLEM OF A FAKE IDENTITY

Other Common Uses of Synthetic Identities

Fraud for Living

Apply for employment or services such as utilities, housing and bank accounts



Credit Repair

Hide from negative credit history in order to appear creditworthy

Other Criminal Activity

Facilitate illegal acts (e.g., money laundering, trafficking or terrorist financing)

THE REAL PROBLEM OF A FAKE IDENTITY

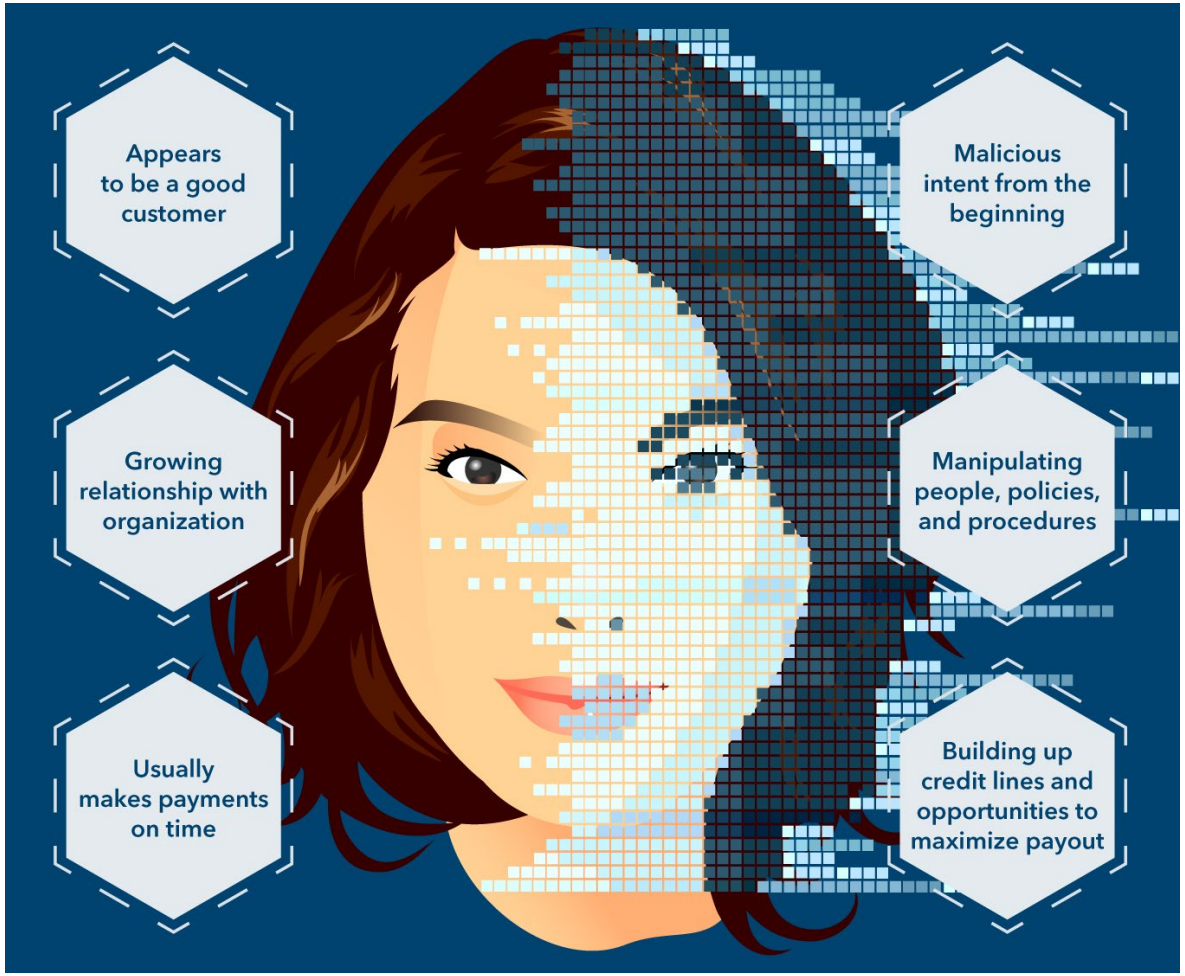
Pervasiveness of Synthetic Identities

Synthetic identities are used to defraud multiple industries (e.g., payments, healthcare and government), making synthetic identity fraud one of the most far-reaching types of fraud.

THE REAL PROBLEM OF A FAKE IDENTITY

Challenges in Detecting Synthetic Identity Fraud

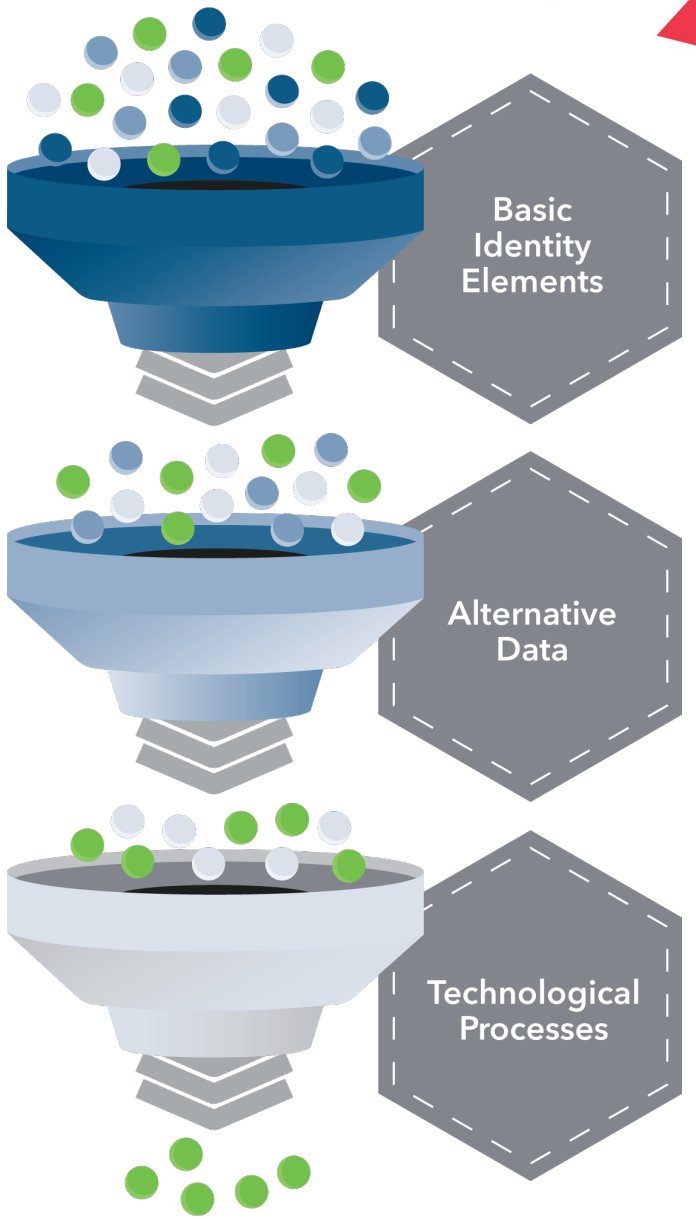
- Onboarding validates information, but not the customer's complete identity
- Customer identity typically not reauthenticated after account opening
- Payment behavior may not indicate fraudulent activity
- Limited ability to detect with conventional fraud models



BEGINNING TO SOLVE THE PROBLEM

How to Fight Synthetic Identity Fraud

- A complex identity requires an equally intricate fraud response strategy.
- Experts suggest that a multi-layered approach is the most effective mitigation strategy.
  - Leverage manual and technological processes to identify common characteristics of synthetic identities
  - Balance these actions to minimize friction and provide a positive customer experience



BEGINNING TO SOLVE THE PROBLEM

Start With Identity Proofing

Identity proofing is verifying the identity presented is legitimate and belongs to that individual.

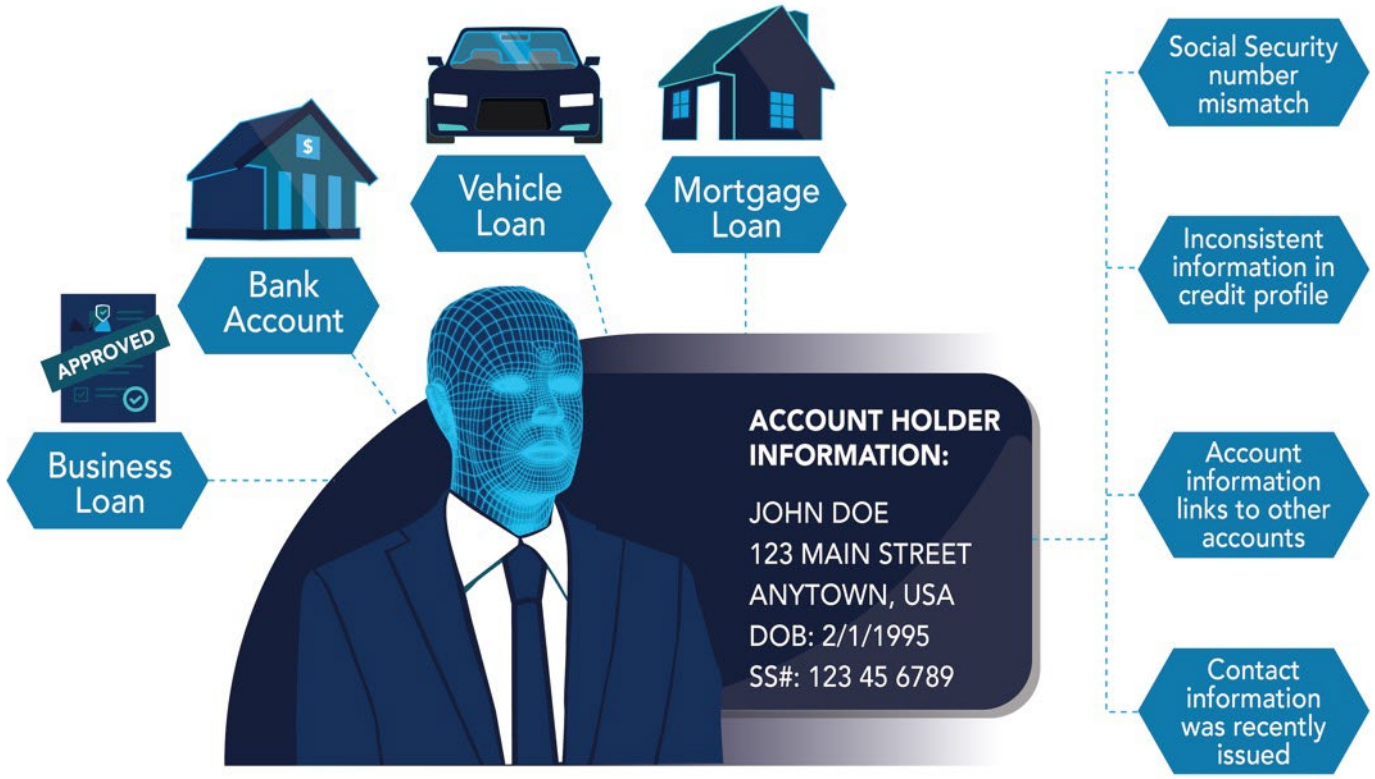
- Continue to perform required customer verification
- Verify foundational identity elements via multiple methods
- Cross-reference identity elements with alternative credit data or additional information that supports proof of life

BEGINNING TO SOLVE THE PROBLEM

Leverage Technology to Maximize Trend Analysis

Artificial intelligence, machine learning, link analysis and other technologies can:

- Complement manual fraud mitigation practices
- Analyze complex data more effectively than humans alone
- Identify relationships across data to help detect common characteristics of synthetic identities



SUPPORTING THE FIGHT AGAINST FRAUD

Industry Resources 'Unmasked'

SUPPORTING THE FIGHT AGAINST FRAUD

Toolkit Module 1 – Synthetic Identity Fraud: The Basics

What makes synthetic identity fraud so attractive?

- Ease of creation
- Frequent data breaches that increase availability of PII
- Credit application process
- Limited verification of identities

SUPPORTING THE FIGHT AGAINST FRAUD

Toolkit Module 2 – How Synthetic Identities Are Used

How do fraudsters take advantage of your portfolio?

- Create multiple synthetic identities
- Submit credit card, DDA, auto/personal loan applications to multiple institutions
- Create profiles that have high chance of avoiding detection
- Ultimately bust out, with no intent to repay

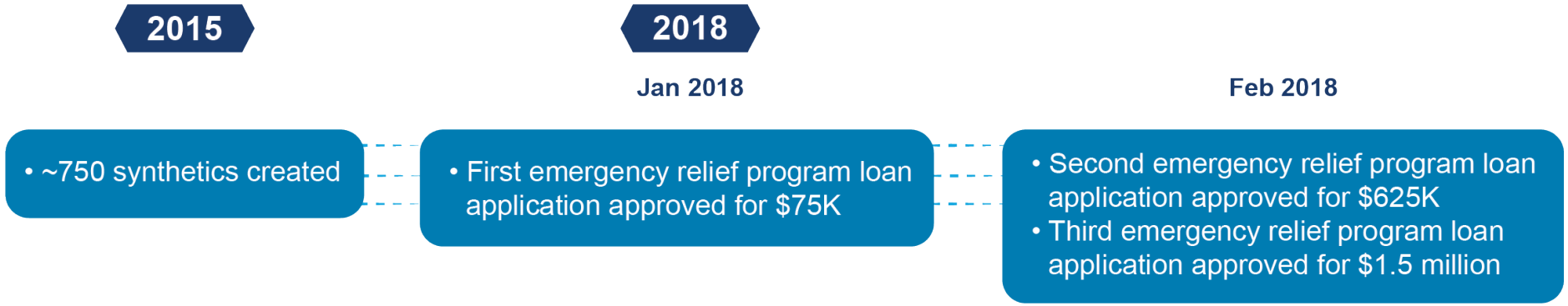
SUPPORTING THE FIGHT AGAINST FRAUD

Toolkit Module 3 – When Synthetics Become a Reality

What are common use cases of synthetics?

- Credit repair
- Emergency relief loan program fraud
- Other criminal activity, such as money mule activity and facilitating trafficking and terrorism
- Fraud for living
- Payment default scheme

Depiction of how fraudsters can take advantage of emergency relief loan program with synthetic identities



SUPPORTING THE FIGHT AGAINST FRAUD

Toolkit Module 4 – Detecting a Synthetic Identity

How can you help mitigate synthetic identity fraud?

- Look for characteristics and suspicious linkages between identity elements that warrant additional investigation
- Increase awareness of synthetic identity fraud across the organization
- Educate customers on how to protect themselves and their children from identity fraud

SUPPORTING THE FIGHT AGAINST FRAUD

Increase Industry Collaboration

- Synthetic identity fraud is not a problem that any one organization or industry can tackle independently.
- Increased collaboration can:
  - Help the industry draw connections to better identify potential synthetic identities
  - Enable discussions to identify potential downstream impacts

SUPPORTING THE FIGHT AGAINST FRAUD

The Federal Reserve's Efforts To Fight Synthetic Identity Fraud

- Encourage use of resources in the Synthetic Identity Fraud Mitigation Toolkit
  - Increase awareness and understanding
  - Foster industry dialogue and collaboration
- Solicit industry and fraud expert feedback
- Further expand the toolkit

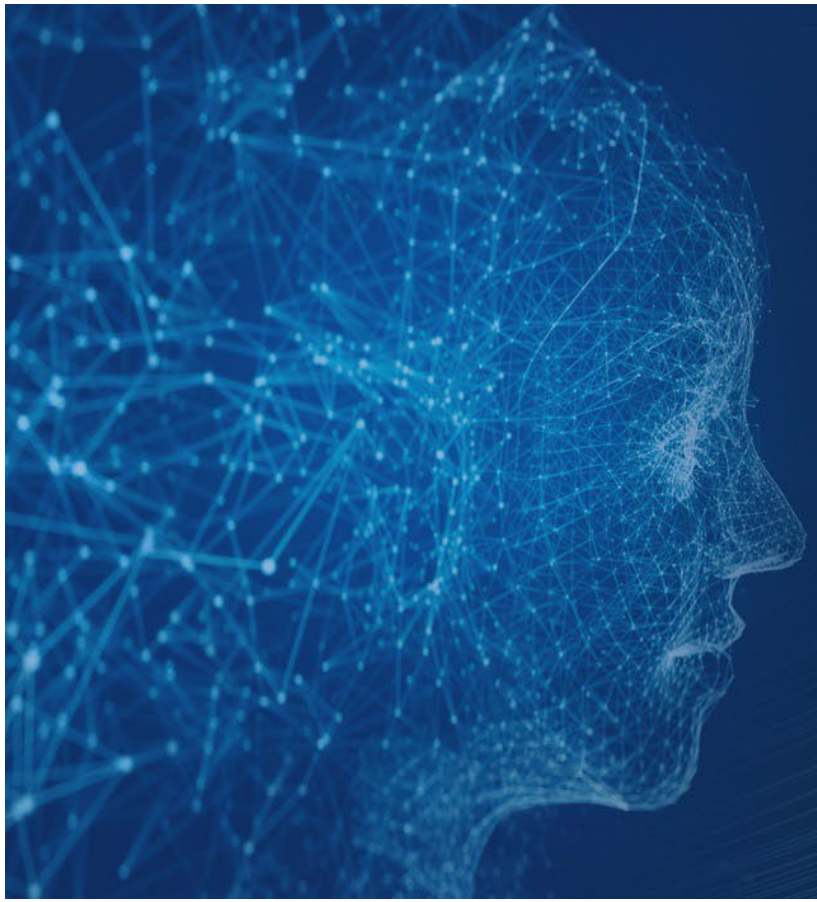
Apply What You Have Learned Today

- Next week you should:
  - Explore the Synthetic Identity Fraud Mitigation toolkit

- In the first three months you should:
  - Utilize toolkit to help further internal education around synthetic identity fraud
  - Gain basic understanding of synthetic identity fraud, how it manifests itself within your portfolio, as well as detection and mitigation opportunities
  - Provide feedback to the Fed on additional resources that would be valuable to have in toolkit

- Within six months you should:
  - Develop plan to evaluate potential synthetic identity fraud risk within your portfolio
  - Utilize consumer section of toolkit to initiate process design to assist customers who fall victim to synthetic identity fraud

Get Connected. Stay Engaged.



FedPaymentsImprovement.org

fedpayments-improvement

@FedPayImprove

FedpaymentsimprovementOrg

Contact us at: SecurePayments@bos.frb.org.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.