THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

Webinar

Synthetic Identity Fraud Mitigation: *One Approach Does Not Fit All*

July 29, 2020

Agenda

Welcoming Remarks

Setting the Stage on Synthetic Identity Fraud

Detection and Mitigation Strategies

Industry Collaboration and Future Outlook

Panel Q&A

Closing Remarks

Industry Experts on Today's Webinar

Jim Cunha - Moderator

Senior Vice President

Federal Reserve Bank of Boston

Greg Woolf

Chief Executive Officer and Founder

Coalesce.ai

Jack Lynch

Senior Vice President and Chief Risk Officer

Payment Systems for Credit Unions (PSCU)

What is Synthetic Identity Fraud?

Synthetic identity fraud is a crime in which perpetrators combine real and/or fictitious identifying information to create new identities.

- **Identity fabrication:** completely fictitious personally identifiable information (PII)
- **Identity manipulation:** slightly modified real PII
- **Identity compilation:** combination of real and fake PII

Sam is a copywriter who is 30 years old, married with two children. He is using an SSN from a 5-year-old child found through a data breach.

Sam is a synthetic identity created using:

Fictitious name

Fictitious date of birth

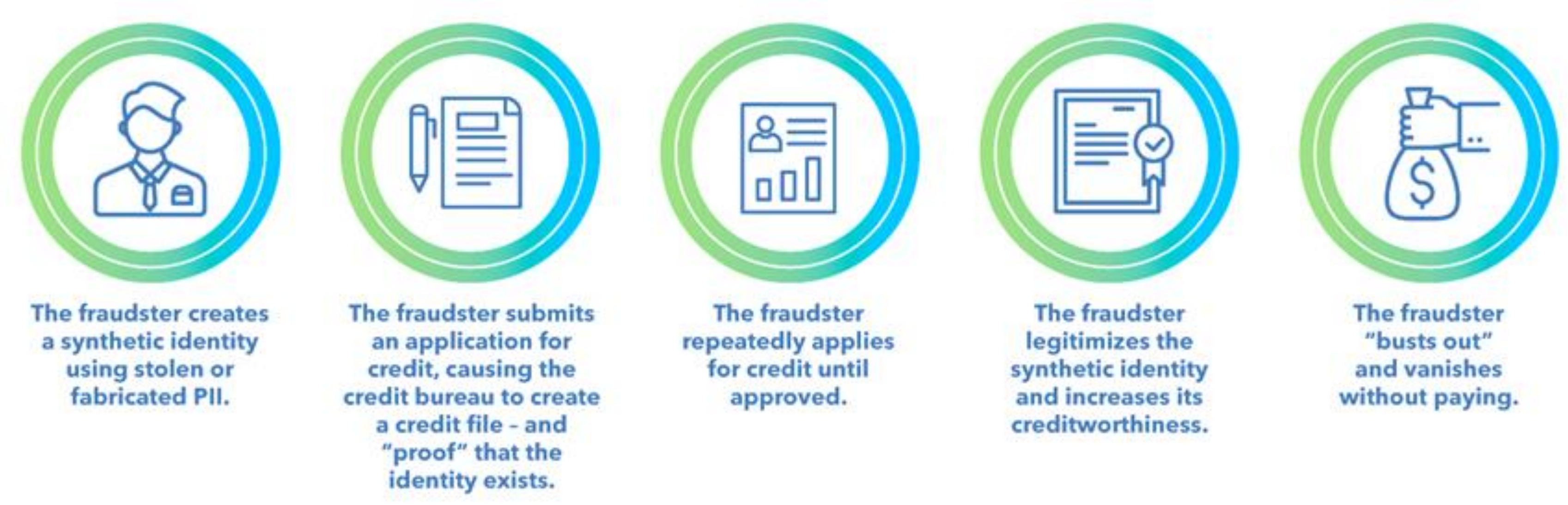
Real Social Security number

Non-residential address (P.O. Box address)

Social media accounts that include images of real people or image library photos found online

Fictitious identity documents

How Synthetic Identities are Used to Commit Payments Fraud



The fraudster creates a synthetic identity using stolen or fabricated PII.

The fraudster submits an application for credit, causing the credit bureau to create a credit file - and "proof" that the identity exists.

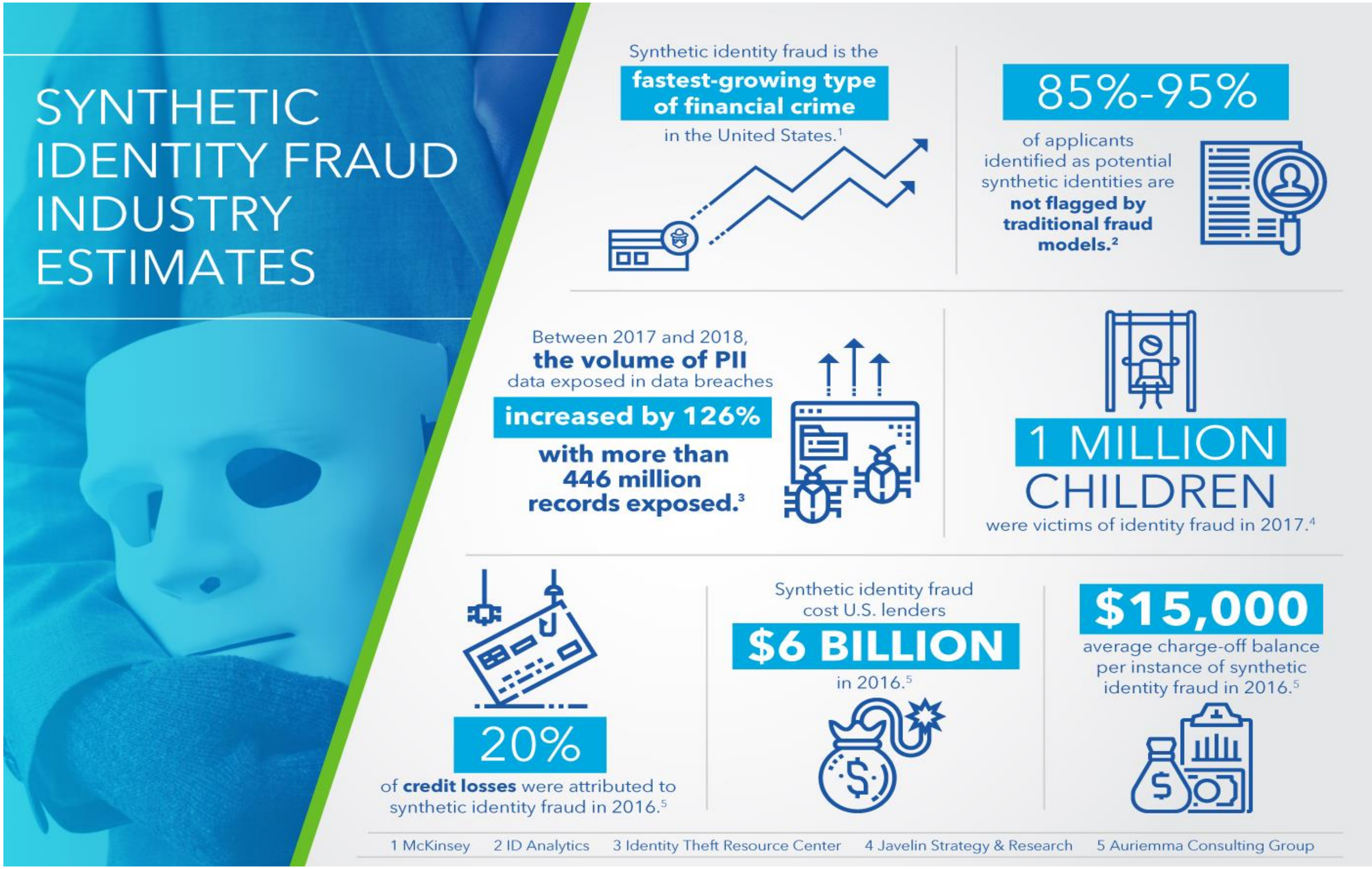
The fraudster repeatedly applies for credit until approved.

The fraudster legitimizes the synthetic identity and increases its creditworthiness.

The fraudster "busts out" and vanishes without paying.

- Synthetic identities are often difficult to detect, as synthetics initially act like financially responsible customers.
- The creation of a credit profile for the synthetic identity helps legitimize the identity, even when credit is initially denied.
- Following the "bust out," the lender has no one to pursue for collections.

The Impact of Synthetic Identity Fraud



SYNTHETIC IDENTITY FRAUD INDUSTRY ESTIMATES

Synthetic identity fraud is the **fastest-growing type of financial crime** in the United States.[1]

85%-95% of applicants identified as potential synthetic identities are **not flagged by traditional fraud models.**[2]

Between 2017 and 2018, **the volume of PII** data exposed in data breaches **increased by 126%** **with more than 446 million records exposed.**[3]

1 MILLION CHILDREN were victims of identity fraud in 2017.[4]

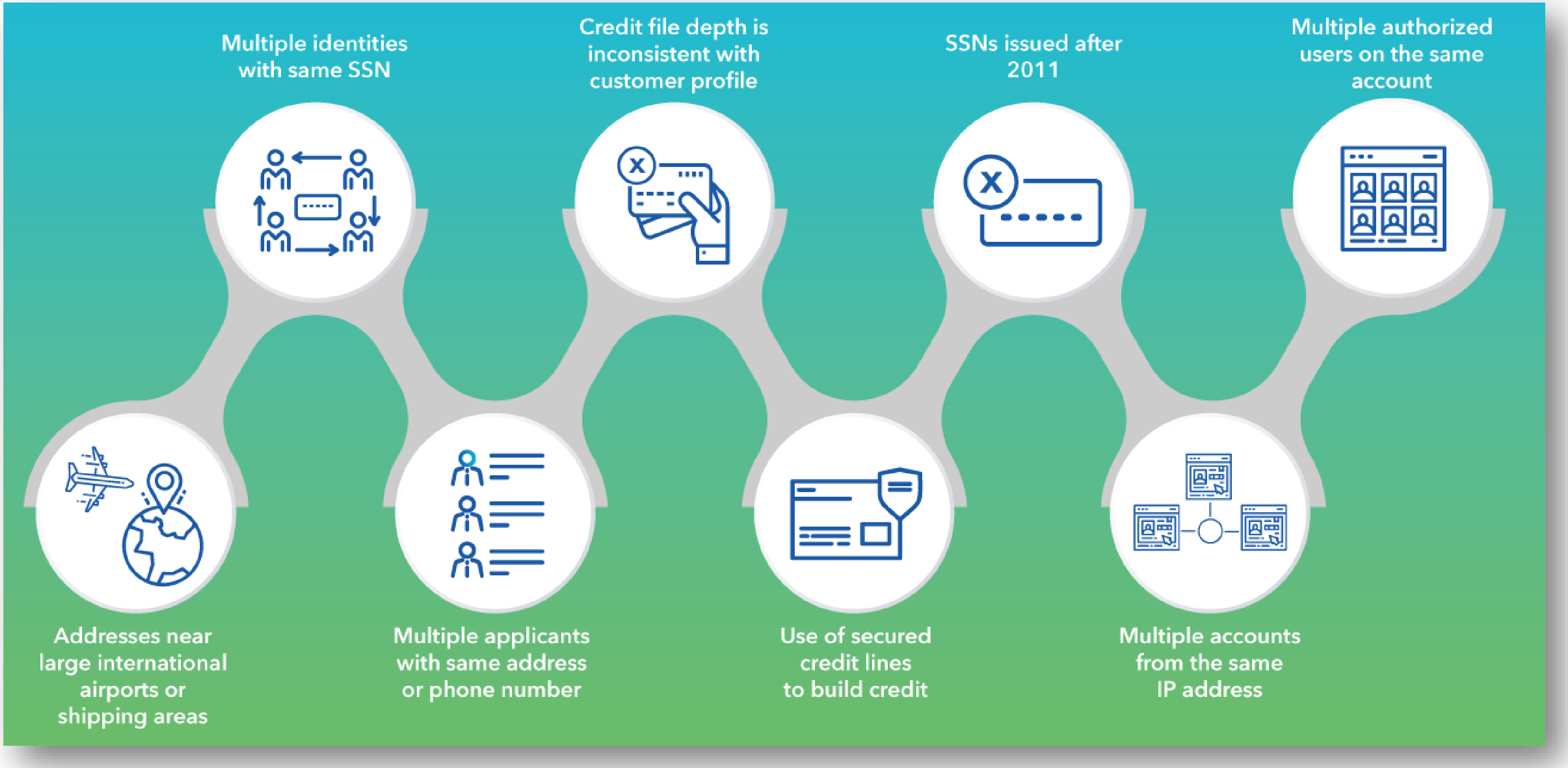
20% of **credit losses** were attributed to synthetic identity fraud in 2016.[5]

Synthetic identity fraud cost U.S. lenders **$6 BILLION** in 2016.[5]

$15,000 average charge-off balance per instance of synthetic identity fraud in 2016.[5]

1 McKinsey 2 ID Analytics 3 Identity Theft Resource Center 4 Javelin Strategy & Research 5 Auriemma Consulting Group

Common Characteristics of Synthetic Identities



Addresses near large international airports or shipping areas

Multiple identities with same SSN

Multiple applicants with same address or phone number

Credit file depth is inconsistent with customer profile

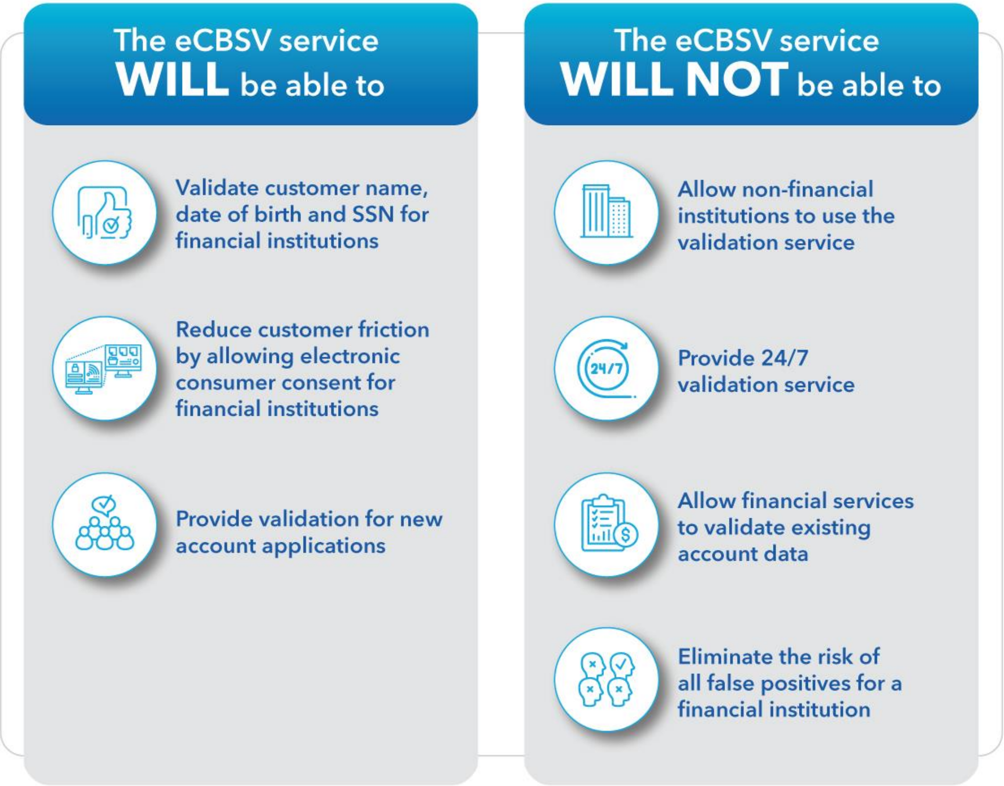
Use of secured credit lines to build credit

SSNs issued after 2011

Multiple accounts from the same IP address

Multiple authorized users on the same account

A New Service to Help with Customer Social Security Number Verification



The eCBSV service **WILL** be able to

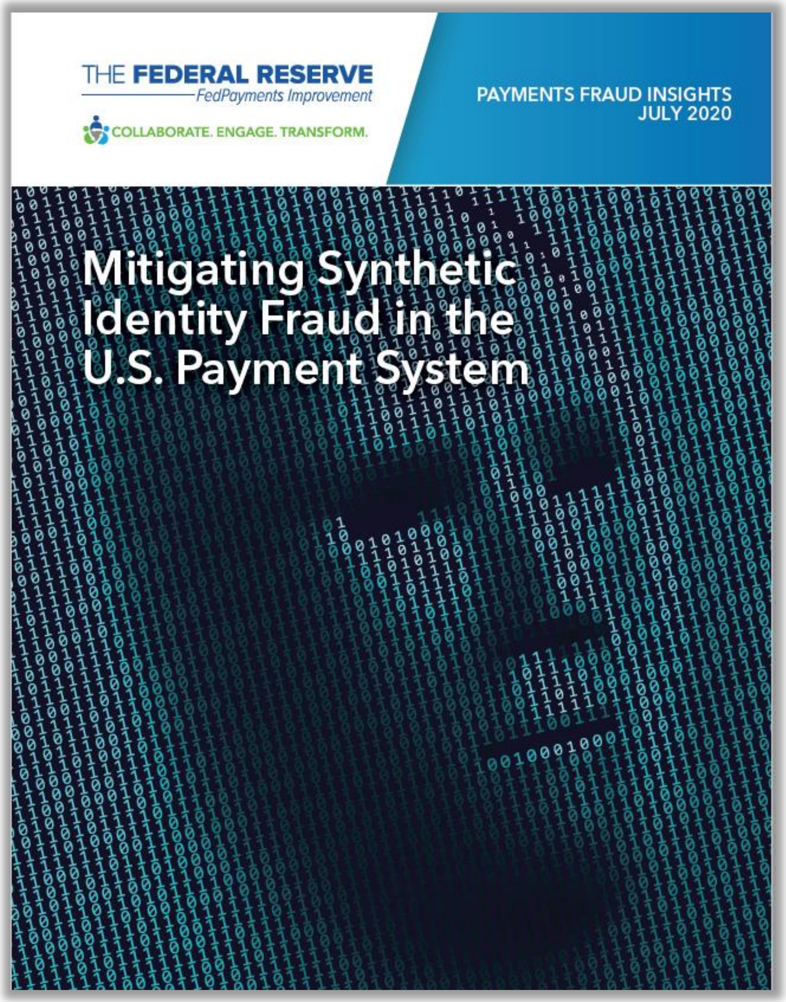
- Validate customer name, date of birth and SSN for financial institutions
- Reduce customer friction by allowing electronic consumer consent for financial institutions
- Provide validation for new account applications

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

The Social Security Administration indicates plans to roll out of the service to a limited number of permitted entities in 2020, with the intent to expand within six months.

Synthetic Identities Require a Multi-Layered Approach to Mitigation



THE FEDERAL RESERVE
FedPayments Improvement
COLLABORATE. ENGAGE. TRANSFORM.

PAYMENTS FRAUD INSIGHTS
JULY 2020

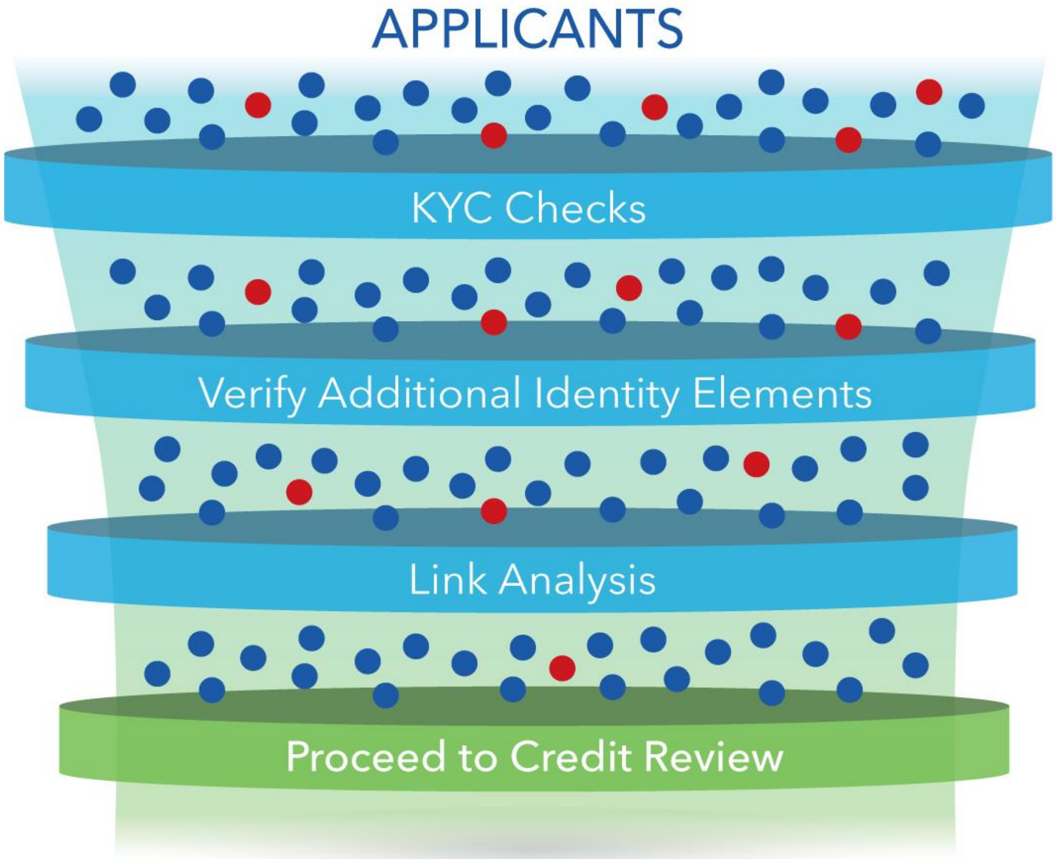
Mitigating Synthetic Identity Fraud in the U.S. Payment System

Key Findings:

- Synthetic identity fraud is not a problem that any one organization or industry can tackle independently.
- A complex identity requires an equally intricate fraud response strategy.
- Changes in the regulatory landscape have influenced industry response
- Experts suggest that a multi-layered approach is the most effective strategy for mitigation.

Multi-Layered Detection and Mitigation

- Continue to perform required customer verification
- Look beyond basic PII elements to gain reasonable assurance of the applicant’s identity
- Leverage manual and technical processes to identify common characteristics of synthetic identities
- Must also be balanced with the customer experience to minimize customer friction



Detection and Mitigation Strategies

Greg Woolf

Chief Executive Officer and Founder
Coalesce.ai

A product visionary, Greg Woolf has more than 20 years of experience founding and running fintech companies that deliver state-of-the-art solutions. He currently heads Coalesce.ai, which has developed an AI platform that improves financial crime detection for financial service firms. Currently, Coalesce.ai is working on a collaborative AI platform to identify and mitigate synthetic identity fraud. Woolf was named IT CEO of the Year by *AI Global Magazine*. The Financial Information Management Association named him a fintech innovation winner. Woolf also has founded an AI think tank – a group of senior executives from prominent global financial institutions and government agencies – to explore how AI can improve the detection and mitigation of fraud in the financial industry.

Coalesce.ai Overview

AI & Machine Learning Company

Big Data AI vs. Scaling the Analyst
User Defined Machine Learning (UDML)

Platform for Financial Crime Detection

SynthID™ focus on Synthetic Identity Fraud
Account Opening / Consumer Lending

AI Think Tank

COALESCE.ai

AI Think Tank

1. Government and Industry Thought Leaders
2. Prioritizing Reputational Risk Leads to Collaboration
3. Advised Congress on Modernizing Financial Crime Detection

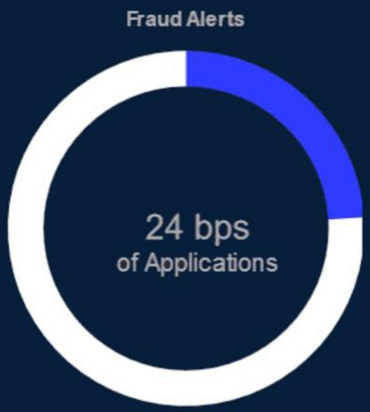
COALESCE.ai

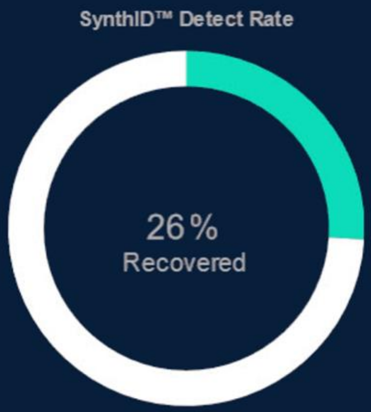
SynthID™ FraudWatch Index

1. Less than 1% of Accounts are Synthetic

2. Account for more than 20% of losses in a consumer loan portfolio

3. Credit losses from Synthetics are 4x the average





Detection and Mitigation Strategies

Jack Lynch

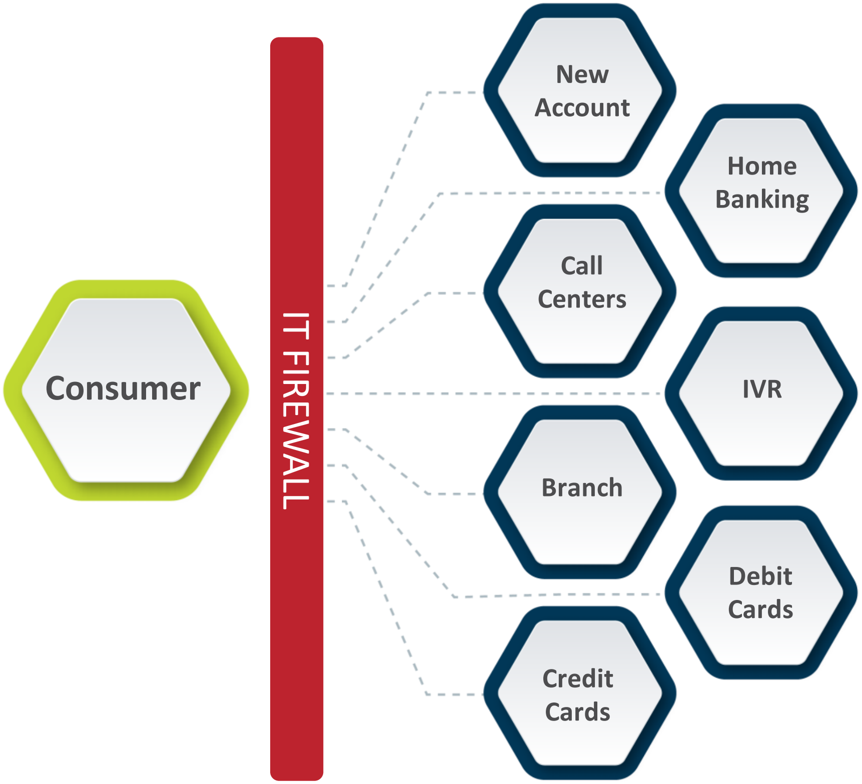
Senior Vice President and Chief Risk Officer
Payment Systems for Credit Unions (PSCU)

President, CU Recovery & The Loan Service Center

Jack Lynch leads PSCU's Fraud and Risk Management Operations area, which provides more than 1,500 credit unions and their members with industry-leading solutions for protection against losses from fraud, lost/stolen accounts, and disputed transactions. He also is president of CU Recovery, which provides delinquency management services and collections training, as well as The Loan Service Center, a PSCU company specializing in delinquency management. Lynch has more than 25 years of leadership experience delivering operational services, project management, client implementations, process re-engineering, account management, training and technology services.

Traditional Fraud Fighting Tactics

Focusing on channel and behavior in that channel



- Neural networks
- Risk Scores
- Decisioning based on consumer transactions
- Limited data based on channel
- Data

Decisioning Based on Event

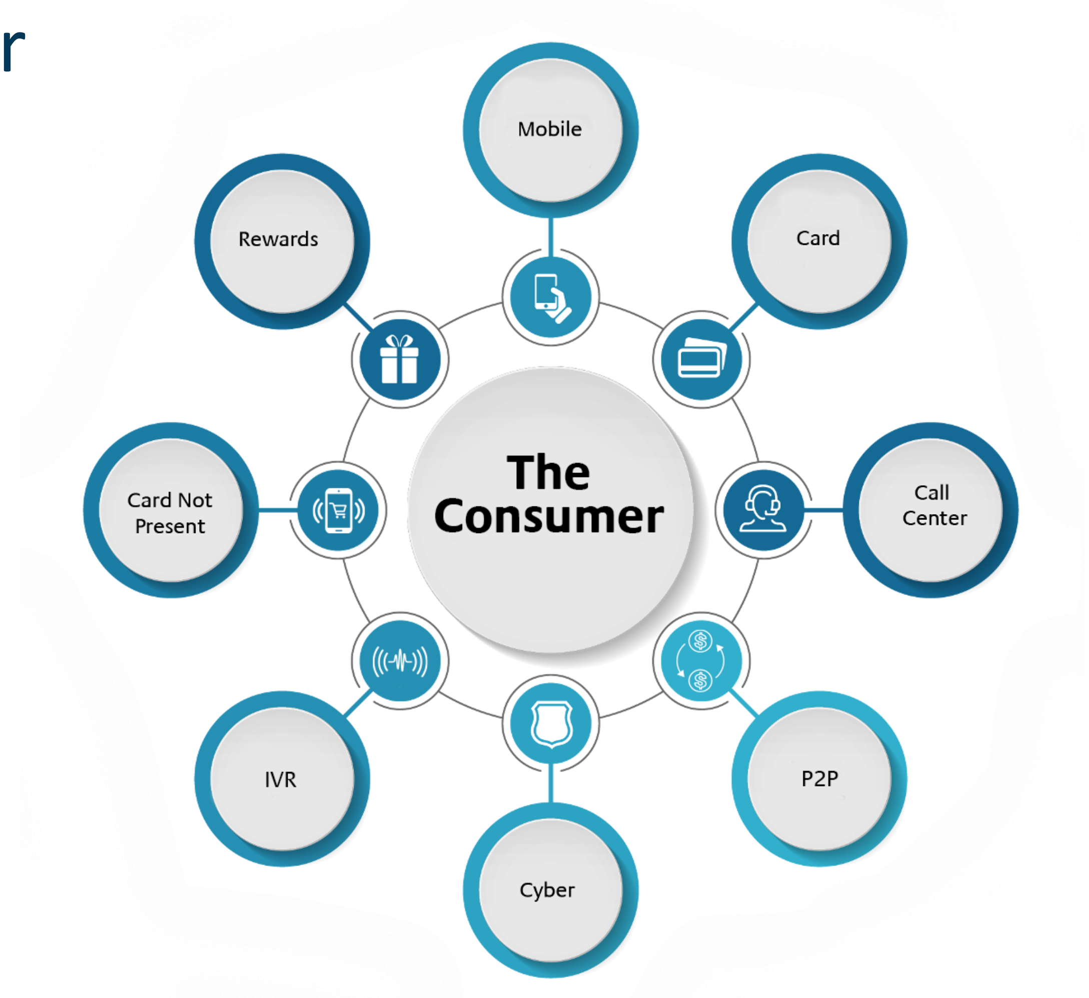
Data NOT Connected

Static Data

Focus on Consumer Interactions Across Channels

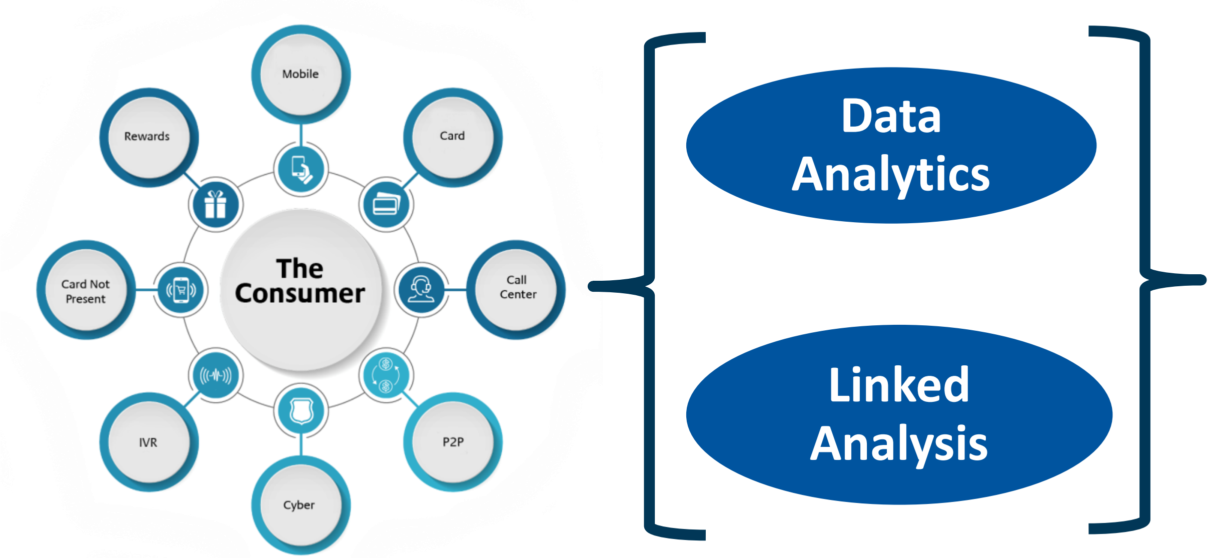
Approach

- Holistic
- Layered



Linked Analysis and Data Analytics

Moving from static data and protecting channels to holistic fraud protection



Data Analytics

Linked Analysis

- Neural networks
- Risk Scores
- Biometrics
- Real Time Data Sources
- Digital Identities
- Authentication data
- AI

Group Discussion:
Industry Collaboration and Future Outlook

Jim Cunha - Moderator

Senior Vice President

Federal Reserve Bank of Boston

Greg Woolf

Chief Executive Officer and Founder

Coalesce.ai

Jack Lynch

Senior Vice President and Chief Risk Officer

Payment Systems for Credit Unions (PSCU)

Panel Q&A

The Federal Reserve's Next Steps on Synthetic Identity Payments Fraud

- Focus on developing a consistent definition of synthetic identity fraud
- Continue ongoing industry education campaign

Learn More and Engage with Us

THE FEDERAL RESERVE
FedPayments Improvement
COLLABORATE. ENGAGE. TRANSFORM.

FedPayments Improvement.org

@fedpayimprove

FedPayments Improvement

FedPayments Improvement

THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

Thank you for joining our webinar!