NCFTA & FiVerity
Security Bulletin – Synthetic Identity Fraud
November 2020 | Issue 01

Advisory on Synthetic Identities used by cyber-criminals to infiltrate financial institutions

This bulletin will help protect financial institutions and their customers from cyber fraud, money laundering and other cyber-crimes. Solutions include detection, prevention and reporting of cyber criminals who use fake identities to infiltrate financial institutions via "shell-personas" to commit crimes.

Target Audience

CEO's, COO's, CCO's, CISO's at financial institutions

Heads of Risk, Fraud, Loss Prevention, Retail Lending, Credit Cards, Cyber Security, Threat Intelligence

Purpose

Awareness, education, and collaborative mitigation action

Notification Request

Financial institutions with a significant digital lending and retail customer presence are encouraged to participate in a Consortium to combat Synthetic Identity Fraud.

Introduction to Synthetic Identity Fraud (SIF)

According to the Federal Reserve[1], Synthetic identity fraud (SIF) has become the fastest-growing type of cyber fraud in the financial sector, projected to cost the industry more than $12bn and account for more than 20% of credit losses[2]. SIF is more sophisticated than basic identity theft, cyber-criminals obtain a combination of falsified and real identity data from the Dark Web to create and cultivate fictitious accounts as a precursor to subsequent fraud and criminal activity.

The sudden increases in stay-at-home banking activity during the Covid-19 pandemic has more than tripled online banking activity[3], compounded with the expected increase in white collar crime[4] has created significant financial, compliance and national security risk for financial institutions. In addition to credit card fraud, loan fraud, and healthcare fraud, law enforcement authorities are concerned that criminals are using SIF accounts as a springboard for more serious crimes such as SIF should also be a cause for concern for more serious crimes such as money laundering or terrorist financing.

SIF is growing rapidly in 2020

SIF schemes are growing at a 25% rate because this type of fraud is often successful for the perpetrators[2]. The cobbling together of real and falsified data makes this fraudulent activity difficult and time consuming to detect.

[1] Federal Reserve Whitepaper Series "Mitigating Synthetic Identity Fraud In the US Payments System"
[2] According to The Auriemma Group Study in 2016, the financial services industry wrote-off $12bn In losses from SIF
[3] Fidelity National Information Services study of 50 largest banks shows a 200% increase in mobile registrations from COVID closing of branches
[4] FBI Statement Before the Senate Judiciary Committee, July 2009, describes a 100% increase in financial fraud during the 2008 recession

SIF accounts are typically seasoned for six to twelve months, systematically building up the size of balances, credit limits, purchases and payments to eventually perpetrate large-scale theft and criminal transactions. SIF fraudsters often employ automation tools to generate thousands of phony identities, fraudulent accounts, and loan applications which overwhelms a financial institution's cyber fraud prevention efforts.

The mandated protection of personally identifiable information (PII) can preclude banks and other financial institutions from sharing intelligence about SIF accounts with third parties, including other financial institutions and law enforcement efforts (in the absence of a warrant), providing cover for SIF fraudsters' criminal activities, and inhibiting detection and prevention efforts.

Beyond Fraud - A Springboard for a Range of Serious Crimes

SIF has been in around for longer than most realize and is often perpetrated by well-funded and highly organized bad actors, including organized cyber-crime rings and foreign nationals acting as a "front" for money laundering, criminal acts, and terrorist activity. The 2008 global financial crisis precipitated an exponential rise in SIF. In February 2013, federal agents in four states arrested 13 individuals associated with a $200 million international bank fraud scheme where the defendants created more than 80 shell companies, 7,000 synthetic identities, and obtained over 25,000 fraudulent credit cards, resulting in 22 arrests and 19 individuals sentenced to prison[5].

> The general lack of awareness in the financial services sector about SIF is partially responsible for SIF schemes effectively evading detection.

According to the criminal complaint, the perpetrators operated a massive international "bust-out" scheme that spanned eight countries, 28 states, and included more than 1,800 drop addresses in the US. The majority of proceeds were used to purchase luxury items and gold, while tens of millions of dollars were laundered to Pakistan, China, Romania, Japan, Canada, and the United Arab Emirates. More recently, in August 2020, the DOJ charged two Florida men in a $3 million Paycheck Protection Program

[5] January 2016: Leader Of $200 Million International Credit Card Fraud Scam Sentenced to 80 Months In Prison

(PPP) loan fraud scheme, where the defendants used shell companies and 700 synthetic identities to defraud five financial institutions and exploit the Coronavirus Aid, Relief, and Economic Security ("CARES") Act[6].

SIF Evades Traditional Cyber Fraud Detection

The general lack of awareness in the financial services sector about SIF is partially responsible for SIF schemes effectively evading detection. Cyber-criminals use commercially available automation tools to generate high volumes of synthetic identities, causing legacy "rules-based" systems and procedures to fail detection in more than 30% of cases[7] due to their lack of accuracy, flexibility, and speed. In response to increased cyber fraud activity, traditional fraud processes are slowing down key business processes like new account verification, resulting in manual intervention in some banks up to 40%, and subpar customer service and responsiveness.

> AI- and ML-powered solutions overlay legacy systems and databases to interpret, distill, and enhance pre-existing rules and improve the effectiveness of fraud and risk detection processes in financial institutions.

Pro-Active Tools for SIF Detection

New solutions based on Artificial Intelligence (AI) and Machine Learning (ML) have emerged that detect SIF activity and cyber fraud from patterns of consumer profiles and activity without PII, thereby removing a key obstacle in proactive SIF fraud detection. AI- and ML-powered solutions overlay legacy systems and databases to interpret, distill, and enhance pre-existing rules and improve the effectiveness of fraud and risk detection processes in financial institutions.

Intelligent automation continuously learns from and builds on the work done by expert fraud analysts by building on uniquely human abilities to find anomalies in non-linear ways. By automatically passing over false positives and bypassing low-risk, alert 'noise', these solutions observe, capture, and enhance analysts' work to create significantly faster, more accurate and

[6] August 2020: Federal prosecutors charge two Florida residents with bank fraud conspiracy for allegedly using synthetic identities to commit crimes, including defrauding banks and stealing over $3 million from Covid-19 relief programs.

[7] FiVerity SIF Fraudwatch Index, September 30, 2020, shows 0.2% of banking accounts are SIF of which more than 30% are undetected

more thorough ways to detect and identify patterns that are the telltale signs of SIF crimes.

Public-Private Collaboration

Communication and information sharing between financial services companies, industry regulators, and law enforcement agencies is critical in the fight against SIF crimes[1]. A recently launched Collaborative program has been designed to be a cross-organizational resource for financial institutions, industry regulators, and law enforcement officials. The Collaboration is a focal point for combining efforts, information sharing, and innovation – all geared toward improving detection and prevention of fraud and other financial crimes while maintaining data privacy of private consumer information. Through a network effect, the AI Collaborative uses secure encryption to share patterns of SIF and known identities of fraudsters without disclosing PII data.

Participants in the Collaboration include the Federal Reserve, the NCFTA, FiVerity, various federal regulators, banks, credit unions, credit card providers, and law enforcement agencies.

About NCFTA

The National Cyber-Forensics and Training Alliance (NCFTA) is a non-profit founded in 2002, focused on identifying, mitigating, and disrupting cyber-crime threats globally. The NCFTA was created by industry, academia, and law enforcement for the sole purpose of stablishing a neutral, trusted environment that enables two-way information sharing with the ultimate goal to identify, mitigate, disrupt, and neutralize cyber threats. Through the NCFTA, private industry and government work together in a neutral, trusted environment (www.ncfta.net).

About FiVerity

FiVerity, Inc. develops AI software solutions that detect new and emerging forms of cyber fraud and deliver actionable, proactive threat intelligence. The company's products meet the unique requirements of financial institutions, including banks, credit unions, and credit card providers. The company's solutions help financial institutions strengthen, streamline, and scale their consumer-facing business processes, such as application processing, credit verification, and customer onboarding (www.fiverity.com).

Further Information

To learn more and participate in the Collaborative Program, please contact the following organizations:

www.ncfta.net	412-802-8000	info@ncfta.net
www.fiverity.com	781-742-7400	info@fiverity.com