Socure

Anatomy of an Alleged PPP Synthetic Identity Fraud Deal

How two people created 700 fake IDs and swindled $3.7 million

By Anthony Winslow | October, 2020

In late August, two South Florida men were arrested on bank fraud conspiracy charges in association with creating more than 700 synthetic identities to steal in excess of $3 million in COVID-19 relief funds.

The scheme dates back to 2017 when the alleged perpetrators created fake identities to establish shell companies and bank accounts at a San Antonio financial institution. From April to July of this year, those same men used those synthetic identities to fraudulently apply for Payroll Protection Program (PPP) loans that were part of the Coronavirus Aid, Relief and Economic Security (CARES) Act. The program represents billions of dollars in forgivable loans for American small businesses struggling because of the pandemic.

Synthetic identities often stem from a combination of real and fake attributes, such as a name and Social Security number, that don't correlate to each other in order to form an entirely new, but fictitious identity. According to a 2018 Wall Street Journal article, synthetic ID fraud is the fastest-growing type of financial crime in the U.S., accounting for 10% to 15% of charge-offs in a typical unsecured bank lending portfolio.

How the Case Unfolded

The 22-page criminal complaint that supports the charges against the South Florida men is based on an investigation by the Federal Deposit Insurance Corporation Office of the Inspector General (FDIC-OIG). Let's break down this information outlining a years-long series of complicated events into digestible segments and associate known synthetic fraud characteristics.

After the synthetic identities were created in 2017 and used to establish accounts at the San Antonio victim bank, the bank became suspicious that a number of these accounts were fraudulent in early 2019. Once categorized as "fraud," the bank used the account information to link to other accounts and identities and found that a number of those accounts were making payments to each other by credit card or convenience check. A spider web visualization of linked accounts emerged which led investigators to presume these accounts were all part of a single scheme. Furthermore, many of these accounts had been opened in the names of incarcerated inmates, who are less likely to be

monitoring their credit profiles. Throughout 2019 and into 2020, some of these accounts continued to transfer money or payments to other linked accounts.

In March, 2020, the United States shut down because of the COVID-19 pandemic. Instantly, millions of U.S. small businesses were thrust into economic crises. On March 27, the CARES Act authorized PPP loans through Small Business Association previously-approved lenders which would be guaranteed by the SBA. Application acceptance to lenders commenced on April 3.

One of the alleged perpetrators wasted no time to bust out. On April 4, a participating lender received a PPP loan application for a company registered to the perpetrator. The application claimed that the company had 11 employees and requested a $60,000 loan.

Later, the Florida Department of Revenue (FLDOR) confirmed there was no record of wages being paid to employees at this organization. Furthermore, at least two of the "employees" were confirmed to be part of the synthetic identities created in 2017.

After signing SBA Form 2483 attesting to the true and accurate nature of the application and acknowledging that making a false statement is a crime, the perpetrator received a wire transfer of $60,000 to his business account from the SBA lender on May 1.

Six days later, the second perpetrator applied for a PPP loan for his shell company through a fintech operation that provides working capital to small and medium-sized businesses. He claimed 33 employees and sought a loan amount of $544,650. He provided his legitimate Florida driver's license as identification. Supporting IRS tax documents showed the company paid identical wages to employees in the same amount for four consecutive quarters—which is highly unusual. Subsequent forensics proved the documents were all created on the same day and never filed. According to SBA records, this loan was made on the same day the application was filed by the fintech's sponsor bank.

After these two instances, the PPP loan applications shifted from businesses "owned" by the perpetrators to companies owned by other individuals. At least two of the synthetic identities created in 2017 used the real names of actual business owners in the state of Florida. This would imply that three years earlier, the perpetrators not only intended to exploit an individual's credentials but that eventually they would use that information to swindle financial aid for an alleged business. At the time, there was no way to predict that a pandemic would occur that created the "perfect storm" for fraud of significant proportions.

On May 9, three days after the second perpetrator received the proceeds for his company's half-million dollar "loan," a PPP application was filed through the same fintech capital firm for a Miami housekeeping business by the "owner" who was one of the synthetic identities referenced above. The application indicated the company had 72 employees and requested $1.4 million. The FLDOR subsequently reported that the company paid no wages in 2019.

The name of the applicant and the business address indicated on the application matched corporation records filed with the Florida Secretary of State's office. On the same day the application was filed, a mail forwarding request was submitted to the USPS which changed the address from the owner's address to the second perpetrator's home address.

On or about May 12, a second sponsor bank for the fintech company wired $1.4 million to a bank account in the name of the business owner.

On or about May 11, a PPP application was filed through the same fintech capital company for a second Florida corporation in the name of the actual business owner, but now known to be a synthetic ID. It sought a loan of $1.7 million and claimed to have 200 employees. The characteristics of this application matched all the others.

The very next day, $1.7 million was wired to an account in the name of the business owner by one of the fintech company's sponsor banks.

In total, these four transactions netted the two perpetrators **$3.7 million**.

How the Perpetrators Were Caught

When accounts were flagged as "fraud" in 2019, we suspect the victim bank reached out to the FDIC-OIG who leveraged breached KBA databases to cross reference associated personally identifiable information (PII.) It allowed them to identify that many of those accounts had been opened in incarcerated inmates' names which were included in the breached databases. At one end of the spectrum, they might be dealing with identity theft and at the other end, it could be synthetic IDs instead. It was by associating some legitimate information that ultimately led investigators to confirm the fraud classification and, more importantly, identify the individuals behind the criminal activity.

The bank itself could see that at least some of these accounts had been transferring money to other accounts which likely supported the assumption that they were part of a single scheme.

It was also likely around this time that investigators determined that the Social Security numbers associated with the bank accounts belonged to minor children and not the inmates whose names were on the account. This could have been the first confirmation that synthetic IDs were created to open those accounts.

One of the perpetrators used his legitimate Florida driver's license with a current address to apply for his own PPP loan. This alone was not sufficient to identify him as a "real" person since synthetic identities are difficult to detect, however it strengthened the overall evidence.

Both of the perpetrators applied for PPP loans for their own fake shell companies and conducted banking activity online from their homes which were linked to static IP addresses. During the criminal investigation, their ISP provider identified the perpetrators and their addresses.

One of the perpetrators filed a mail forwarding order for the legitimate owner of one of the businesses for which a PPP loan was secured where mail was redirected to his home address.

Purchases made using the synthetic ID credit cards were linked to loyalty accounts in the real names of one of the perpetrators and a co-conspirator.

As PPP loan funds hit these synthetic accounts which were likely already flagged as suspicious, the high balances certainly exceeded prior activity and should have attracted the attention of bank officials.

Finally, a third co-conspirator was identified but never charged as far as we can determine. This person initiated wire transfers between the fraudulent accounts and accessed PPP loan applications online from his or her home. We suspect this person was approached about cooperating with investigators and ended up verifying the identity of the perpetrators and confessing to the scheme for which he or she was granted leniency.

How the Scheme Ties to Known Synthetic Fraud Characteristics

The events that took place over the course of this elaborate scheme can be tied directly to several known characteristics of synthetic identity fraud. For example:

Synthetic identities can go for long periods of time without detection: More than 700 synthetic accounts were established with the victim bank in 2017. The bank did not become suspicious about those accounts for two years. Apparently, the perpetrators established a history of using the fraudulent accounts responsibly before becoming delinquent and, even then, perhaps just looked like a person having financial problems before they were flagged as criminal.

Reliance on stolen PII and disparate elements of real identities repurposed from different victims: According to the Identity Theft Resources Center, there were 446 million breached records available around the time that the synthetic identities were created in 2017. It included compromised inmate and consumer data that was available for sale on dark web marketplaces. The perpetrators even relied on government databases to identify legitimate business owners. The probable goal was for the synthetic identities to look more realistic, and it worked for a while.

Fake IDs were employed: Bank accounts cannot be established without proof of identification. No doubt, the perpetrators utilized fake identification to establish these synthetic ID depository accounts.

One or more of the accounts likely busted out: As previously stated, the victim bank became suspicious in early 2019. The likely reason is that one or more of the accounts "busted out." A bust out is a type of credit card fraud where an individual applies for a credit card, establishes a normal usage pattern and repayment history, and then maxes out the available credit with no intention of repaying the balance.

Multiple applications were filed and crossover transactions occurred from the same IP addresses: Investigators documented that the four referenced PPP applications and bank account transfers from multiple synthetic accounts came from just three static IP addresses tying back to the two perpetrators and a co-conspirator.

Children's Social Security numbers were used for many of the synthetic identities: Children's data is often associated with synthetic fraud because they do not have easy access to their credit reports nor are those reports checked very often.

Credit requests were initially nominal and then increased in value: The perpetrators followed the known synthetic fraud approach of applying for nominal credit initially to see if it is approved before moving on to more and more significant amounts. In this case, the initial ask was $60,000, followed by $545,000, followed by $1.4 million, and finally, $1.7 million.

How to Mitigate Synthetic Identity Fraud

Financial institutions need to mitigate synthetic fraud for many reasons, but among the most important include: avoidance of KYC non-compliance fines, monetary losses from unpaid credit balances and ongoing operational expenses, mistakenly labeling synthetic fraud as bad debt, and reputational damage to their brand.

Technological innovation can help FIs verify customers at digital entry points and other stages in the user lifecycle. The best defense against synthetic fraud is to rely on a multi-layered approach that looks beyond basic PII elements and leverages advanced analytics and diverse, deep data sets to gain assurance of the applicant's identity. Furthermore, deploying artificial intelligence and machine learning to detect synthetic identities creates efficiencies for FIs and avoids manual reviews and human error.

Socure's Sigma Synthetic Fraud solution tackles synthetic identity fraud through feature engineering and data source analysis. It used both supervised and unsupervised machine learning models to derive a common definition of synthetic identity fraud, upon which Socure developed classification models that have proven effective in combating this elusive type of fraud. Sigma Synthetic Fraud has achieved 97.3% under the ROC curve with an auto-fraud capture rate of 90% in the riskiest 3% of users.

Sigma Synthetic Fraud is part of Socure ID+, an integrated identity verification platform, alongside Sigma Identity Fraud, Compliance and DocV. Sigma Identity Fraud delivers a multi-dimensional view of identity risk with ML models that are trained with feedback data from a consortium of clients to tackle targeted fraud patterns and produce real-time, actionable risk scores and reason codes. Compliance addresses AML/BSA compliance with over 90% auto acceptance for KYC and lower false positives by 80% for Watchlist enforcements worldwide. DocV accelerates verification of government-issued IDs with analytics-based document authenticity and facial liveness checks.

This powerful module effectively manages synthetic fraud risk without slowing down new business growth or turning a blind eye to potentially risky accounts. When applied at account enrollment or to an existing portfolio, Sigma Synthetic Fraud quickly assesses the risk of synthetic fraud and renders a decision in a fraction of a second. Sigma Synthetic Fraud and all Socure products are accessible via one single API that powers the entire Socure ID+ platform.

For more information about Sigma Synthetic Fraud, please contact sales@socure.com.

Socure