SentiLink

July 13, 2023

The Honorable Roger Williams
Chairman
Committee on Small Business
U.S. House of Representatives

The Honorable Nydia Velazquez
Ranking Member
Committee on Small Business
U.S. House of Representatives

Dear Chairman Williams and Ranking Member Velazquez:

On behalf of SentiLink, I am pleased to submit this statement for the record for your hearing titled "*Stolen Taxpayer Funds: Reviewing the SBA and OIG Reports of Fraud in Pandemic Lending Programs*." SentiLink works with over 300 financial institutions to prevent synthetic fraud, identity theft, and other emerging forms of first party fraud at the point of account origination. We were also the first company in history to use the Social Security Administration's Electronic Consent Based SSN Verification service (eCBSV) to validate account application data.

The federal government's response to the pandemic saw unprecedent volumes of money moving at a very rapid pace to consumers and businesses. As a rule, when any amount of money moves electronically, there is always the possibility that a fraudster is either behind it or hoping to divert it for themselves. When trillions of dollars are moving, that threat grows exponentially.

With the benefit of hindsight, we have been able to analyze our own proprietary data as well as publicly available information to draw conclusions that we hope can help shape future policymaking decisions. Overall:

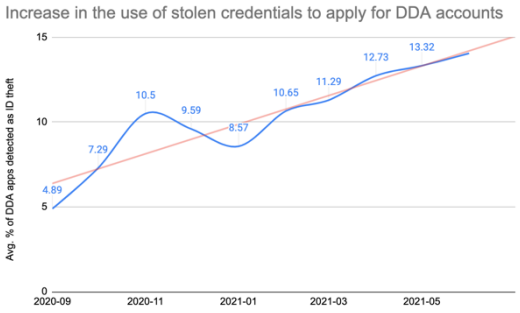
- Tens of billions of taxpayer dollars were misappropriated or outright stolen by scammers and identity thieves.
- Policy decisions prioritized speed –i.e., getting stimulus funds to consumers and businesses – over identity due diligence.
- Achieving the policy objective of speeding funds to legitimate recipients, while simultaneously preventing widescale fraud, was entirely achievable. Had the U.S. government placed a priority on the need to use readily available technology to ensure funds were being delivered to the correct recipients and not identity thieves or synthetic identities, the fraud losses incurred would have been significantly less.
- The use of synthetic and stolen identities to open checking accounts to launder ill-gotten pandemic relief funds remains a problem for the financial industry broadly, as those accounts continue to show clear signals of poor performance and additional fraudulent behavior.

<u>Identity Theft at the Heart</u>

We believe the widescale, organized theft of pandemic relief payments relied on applications to the various stimulus programs using stolen identity information, with fraudsters using the name, date of birth, Social Security number, and address of their victim to first establish a bank account. With a deposit account opened, fraudsters then used the same stolen identity information to apply for government relief funds, to be remitted to the fraudulently opened checking account. When the funds

were received, they could be laundered through a myriad of other financial accounts such as other deposit accounts, peer-to-peer payment services or cryptocurrency platforms.

Based on our analysis to date, we believe a significant portion of this fraud found its way into the banking system by way of checking accounts (DDAs) created with stolen identities. An analysis of data from a sample of SentiLink partners illustrates the growing incidence of DDA account applications using stolen identity credentials during this period.



From September, 2020, to June, 2021, the percentage of applications for DDAs identified by SentiLink as using stolen identities increased 187%.

Many of the identity theft victims in these instances may not be aware that their credentials have been compromised in this way. Others may have received a welcome package from their "new" checking account provider in the mail sometime later, by which time the fraudster would have already used online banking to exfiltrate and launder the stolen funds.

More recently, SBA data on all PPP loans originated during the pandemic has been made available to the public through a Freedom of Information Act (FOIA) request. While our analysis of this data is ongoing, many loans were made to businesses that do not exist. Further, individuals that received many of these PPP loans show a clear propensity to commit fraud generally. Our initial analysis suggests the recipients of loans made by the five lenders affiliated with Blueacorn and Womply – two fintechs noted in the Select Subcommittee on the Coronavirus Crisis Staff Report as having lax fraud controls -- are 5X-20X more likely to subsequently commit additional fraud against other financial institutions, such as ACH and check fraud.

Synthetic Identity Fraud

Specific to synthetic identity fraud, SentiLink examined a sample of 25 known synthetic identities who applied to the Small Business Administration for COVID Economic Injury Disaster Loan (EIDL) loans between April and August 2020.[1] Twenty-one of these identities were first party synthetics, which means they were real people using Social Security numbers (SSN) that didn't belong to them. Four of the identities were third party synthetics, which means they were totally fabricated identities. Third party synthetic identities are often created by organized crime groups with malicious intent.

For the most part, the synthetic identities who applied for credit with the SBA were quite established. Most had inquiries and tradelines dating back to 2018. Only three were created in early 2020.

While this analysis of synthetic identities used to apply for EIDL loans was only based on a relatively small sample, it is clear evidence of abuse of federal COVID relief programs by synthetic identity

[1] We assume identities with an inquiry to the SBA between April and August 2020 were applying for an EIDL loan. The EIDL does have two other programs, military reservist and physical damage loans, but there are limitations on who can apply, and less likely that inquiries during this short time period were related to them.

criminals.[2] We believe this pattern manifested itself across the range of federal small and medium-sized business relief programs. Entirely fictitious businesses, or real businesses with fictitious employees used to apply for loans, is a known practice among fraudsters, which was unquestionably accelerated in the context of COVID relief programs.

Thank you for holding this hearing. The use of stolen and synthetic identities to open financial accounts is not new. U.S. financial institutions that onboard new customers digitally are required to have rigorous controls in place, many of which enable identity verification in real-time. The policy mistakes inherent in the government's pandemic relief response provide a valuable learning opportunity as it relates to the importance of identity verification: Had the U.S. government incorporated solutions to detect stolen and synthetic identities when distributing COVID relief funds, the fraud losses incurred would have been significantly less.

We appreciate the opportunity to provide these comments and look forward to engaging with you and your colleagues to advance policy solutions that protect American consumers and businesses from identity crimes.

Sincerely,

Jason Kratovil
Head of Public Policy and External Affairs

[2] For example, see "Defendant Pleads Guilty to Stealing $24 million in COVID-19 Relief Money Through Fraud Scheme that Used Synthetic Identities," US Department of Justice, June 29, 2021. Accessed at: https://www.justice.gov/usao-sdfl/pr/defendant-pleads-guilty-stealing-24-million-covid-19-relief-money-through-fraud-scheme.