SentiLink

September 30, 2021

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
U.S. House of Representatives

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives

Dear Chairwoman Waters and Ranking Member McHenry:

On behalf of SentiLink, I am pleased to submit this statement for the record for your hearing titled "Oversight of the Treasury Department's and Federal Reserve's Pandemic Response." SentiLink provides industry-leading solutions to prevent synthetic fraud, identity theft, and other emerging fraud vectors at the point of account origination. I am also proud to note that SentiLink was 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.

Unfortunately, from unemployment insurance[1] to Paycheck Protection Program (PPP) and Economic Impact Payments (EIP)[2], the execution of these programs demonstrated how inadequate the government's choices were when it came to identity verification. Numerous reports highlight how the many stimulus and relief programs created to prop up the economy became target-rich environments for people seeking to commit fraud. Tens of billions of taxpayer dollars were misappropriated or outright stolen by scammers and identity thieves. While the need to disburse funds quickly made sense from a stimulus perspective, as one example was reported: "To speed money to struggling businesses, lawmakers required the SBA to take applicants' word that they were eligible for the money—a requirement that SBA Administrator, Jovia Carranza, has called lowered guardrails against fraud."[3]

---

[1] *See* "DOL-OIG Oversight of the Unemployment Insurance Program," June 10, 2021, estimating that $87.3 billion in UI benefits may have been paid improperly, "with a significant portion attributable to fraud." Accessed at: https://www.oig.dol.gov/doloiguioversightwork.htm.

[2] *See* "Implementation of Economic Impact Payments," Treasury Inspector General for Tax Administration, Report 2021-46-034. May 24, 2021. This report concludes that as of July 16, 2020, the IRS had issued "more than 4.4 million EIPs totaling nearly $5.5 billion to potentially ineligible individuals."

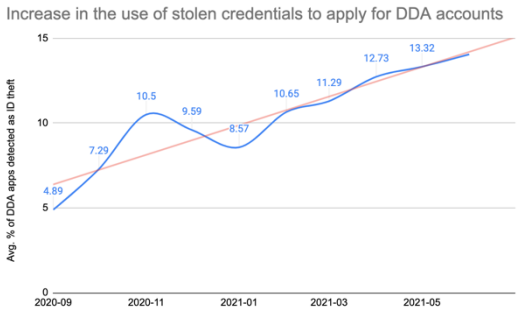
[3] "Phantom Companies got more than $1 billion in Coronavirus Aid," Bloomberg Business. Accessed at: https://news.bloombergtax.com/daily-tax-report/phantom-companies-got-more-than-1-billion-in-coronavirus-aid

SentiLink

Identity Crimes at the Heart

We believe this 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.

Our analysis also suggests evidence of both the use of "money mules" – a scheme in which fraudsters lure unsuspecting consumers into using their personal ID and bank account information to accept criminal proceeds into their account and transfer these funds on the fraudster's behalf.

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.[4] 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.

[4] We are assuming 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.

SentiLink

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 criminals.[5] 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. 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

[5] 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.