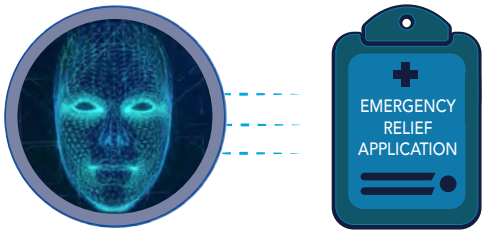
USE CASE: EMERGENCY RELIEF LOAN PROGRAM FRAUD

OVERVIEW

Synthetic identity fraud has continued to evolve over the past several years and fraudsters are quick to respond to significant world events (e.g., natural disasters and global pandemics) and exploit the situation. Fraudsters take advantage of these events by leveraging established synthetic identities that were lying in wait for the right time to cash out.



Some of the fraudsters' attempted targets included emergency relief loan programs aimed at helping businesses or individuals during challenging times.

The following use case depicts how a group of fraudsters leveraged synthetic identities for both individuals and business entities to defraud an emergency relief program.

USE CASE: BUSINESS LOAN SCAM

Two fraudsters created more than 750 synthetic identities – some of which were used to fraudulently obtain millions of dollars from an emergency relief loan program.

As is often typical in synthetic identity fraud, the groundwork for this fraud scheme was laid years earlier. The fraudsters involved in this case began cultivating the synthetic identities back in 2015 and used these identities to establish shell companies[1] and bank accounts at a financial institution. The fraudsters created the identities by using stolen Social Security numbers (SSNs) and creating or pairing the SSNs with other key information, such as name and date of birth.

[1] *A shell company is an incorporated company that possesses no significant assets and does not perform any significant operations. Shell companies have legitimate uses but are often used by fraudsters for nefarious purposes to launder money, facilitate fraudulent payments and make illicit funds and activity appear legitimate. Source:* ***Money Laundering | Wex | US Law | LII / Legal Information Institute (cornell.edu)***

USE CASE: EMERGENCY RELIEF LOAN PROGRAM FRAUD

Below are some examples of the synthetic identities created by the fraudsters:

Initials of Name on Fraud Account	Synthetic Identity Number	Identity Information
N.C.	SID #1	SSN for SID-1 was assigned to an individual with a different name and date of birth (DOB). SID-1 was born in 2001.
D.B.	SID #2	SSN for SID-2 was assigned to an individual with a different name and DOB. SID-2 was born in 2005.
D.C.	SID #3	SSN belongs to an inmate sentenced to life imprisonment, who has been in custody since April 2002.
B.H.	SID #4	SSN for SID-4 was assigned to an individual with a different name and DOB. SID-4 was born in 2009.
D.S.	SID #5	SSN for SID-5 was assigned to an individual with a different name and DOB. SID-5 was born in 2000.
M.P.	SID #6	SSN for SID-6 was assigned to an individual with a different name and DOB. SID-6 was born in 2005.
D.B.	SID #7	SSN for SID-7 was assigned to an individual with a different name and DOB. SID-7 was born in 2004.
J.B. 1	SID #8	SSN for SID-8 was assigned to an individual with a different name and DOB. SID-8 was born in 2003.

USE CASE: EMERGENCY RELIEF LOAN PROGRAM FRAUD

Three shell companies were then created leveraging three of these synthetic identities. The fraudsters leveraged these synthetic identities and shell companies to fraudulently apply for loans as part of the emergency relief loan program over the following timeline:

- **January 2, 2018:** Fraudulent business #1 submitted a loan application request for $75,000. This application contained 15 synthetic identities on the listed payroll to increase the amount of funding received. On January 5, 2018, fraudsters received the first wire transfer of $75,000 to the business account.

- **February 15, 2018:** Fraudulent business #2 submitted a loan application, this time requesting $625,000 In funding. The application listed 50 employees on the payroll, all of which were synthetic identities. To help authenticate the application, one of the fraudsters provided a legitimate state driver's license as proof of identification but provided fictitious IRS tax documentation on employee wages. The application was approved the same day it was submitted.

- **February 22, 2018:** Fraudulent business #3 submitted a loan application, requesting $1.5 million for a housekeeping business listing 100 employees, all of which were confirmed to be synthetic identities. On February 25, $1.5 million in funding was dispersed to the fraudsters.

These identities sat dormant for years before they were used to apply for these emergency relief loans and serve as examples of the magnitude of a fraud attack possible during a significant world event. The fraudsters were able to conduct this fraud by leveraging more than 750 previously created identities. The fraudsters cultivated these identities and kept them in good standing for years while waiting for the perfect opportunity to conduct a quick cash grab. This cultivation is commonly known as "farming" a synthetic identity. Unlike identify theft, there is typically not a complaining victim notifying an associated financial institution or credit bureaus about suspected fraud. This is because during the "farming" stage, the activity associated with the SSN is typically positive and goes undetected by the rightful owners of the SSNs in use. In some instances, the rightful owners – such as children – are not actively using or monitoring their credit. Therefore, these accounts can go undetected for years. Accordingly, fraudsters gravitate toward using synthetic identities due to their potentially high-dollar yield and low probability a victim will come forward.

USE CASE: EMERGENCY RELIEF LOAN PROGRAM FRAUD

AFTERMATH

Prior to determining the owners of these accounts were synthetics, a bank had identified suspicious activity on some of these accounts. With additional investigation, it was determined that these accounts were opened in the name of incarcerated individuals, ultimately uncovering approximately hundreds of suspicious accounts opened under a synthetic identity.

This use case serves as an example of the significant dollar impact that synthetic identity fraud can have and how fraudsters are ready to act with these identities at just the right moment. Synthetic identities are created and introduced into the payment system and not necessarily used immediately but are groomed to be ready for use at the fraudster's discretion.