Synthetic identities

Marius Frunza • IntelBlitz • 5 mins read • Nov 30, 2020

Synthetic identity fraud does not require to steal the identity of another person. A synthetic identity uses various data from several persons. For example, a driver licence from one person, proof of address from another person and a social security number or tax identifier from a third person can be compiled into a new identity. A synthetic identity can be engineered using both real and fake data. The person behind this synthetic identity is fictitious and does not exist in reality.

An identity does not require a life

Because part of the info behind a synthetic identity is real, screening systems have a hard time detecting the scam. This is also explained by the fact that information concerning individuals is harboured in siloed unlinked databases. For instance, the information concerning tax identifiers, social security numbers, passport series and phone numbers are in most countries managed by different administrative entities, with different operating models and different data-warehouses which do not talk to each other. Criminals use a piece of infomration about a real person and can obtain other documents, including IDs, birth certificates, passport, open bank accounts or register businesses.

With the digitalisation of banking services and public administrative processes, an individual can apply for a bank account, a passport or a taxpayer number without having any physical contact with a representative of an administration or bank. The coronavirus pandemic accelerated this trend, thereby increasing the risk related to synthetic identity fraud.

Once created, a synthetic identity is brought to life by a series of actions including some which would not require an IDs:

- Registering to conferences or events
- Booking hotels in various location across the world
- Purchasing travelling tickets for trains and busses
- Creating content on social networks and social media. Facebook allows its users to indicate the place and the activity they are doing at a given time (the ”check-in” feature)
- Building websites related to a business or a professional activity
- Creating CVs on professional platforms like Linkedin

Synthetic identities are used for opening of new bank accounst with the primary intent to commit fraud (also called the new account fraud). The synthetic identities are not only used for credit card theft or application fraud. The scammers use them in other scams that do not require a formal ID check on behalf of the authority. For example, the synthetic identity issues appeared in many fraudulent ICOs(Initial Coin Offering) in the cryptocurrency universe. Most ICOs did not require a formal company to be incorporated, and ICO platforms did not vest the projects. Thus, many fraudulent ICOs took place, the profiles of the project founders being synthetic fake identities.

CEO fraud is another example of crime using the principle of synthetic identity fraud. CEO fraud is known as Business Email Compromise (BEC) and refers to a crime where a criminal creates a synthetic identity of a company CEO or a senior executive in a company. By pretending to be in a high corporate role, the criminal aims to extract funds from a victim or to obtain information that could potentially result in illegal financial gains. For building this image,, scammers employ social networks like Linkedin or Facebook, posting references to their professional activities. The online content and social networks provide them also with leads about the potential victims and the organisation to which they belong. CEO fraud has the following steps:

a. The con-artist creates a synthetic profile representing a CEO, a senior executive or a lawyer. The new synthetic person has fake online profiles, websites and fake corporate email addresses. If a criminal wants to appear as an executive in a big corporation, emails similar to the official email of that corporation will be used. (ie. @jpmorganoffice.com instead of @jpmoragan.com). Criminals also pretend to be senior managers in tax authorities, and they use email version that would sound like the real ones. For instance, if they claim to be from the British customs, they could use emails like @hmrc-omline.co.uk instead of @hmrc.co.uk.

b. Criminals choose their victims carefully. They target both individuals and corporates. In the corporate world, criminals can target legal, accounting or human resources departments to get information or claim a refund.

c. Scammers start campaigns of phishing and cold-calls and solicit victims to wire monies or transfer confidential information. The money transfers are not always the primary goal. Extracting personal information from victims can help criminals to pursue and develop other frauds. Obtaining ID or passport numbers can be useful for creating different synthetic identities.

d. When criminals reach their goal, they erase all information related to their synthetic identities of CEO.

"I hate to use the word light fraud—there's really no distinction—but in comparison to what I ultimately started doing, it was definitely light.."

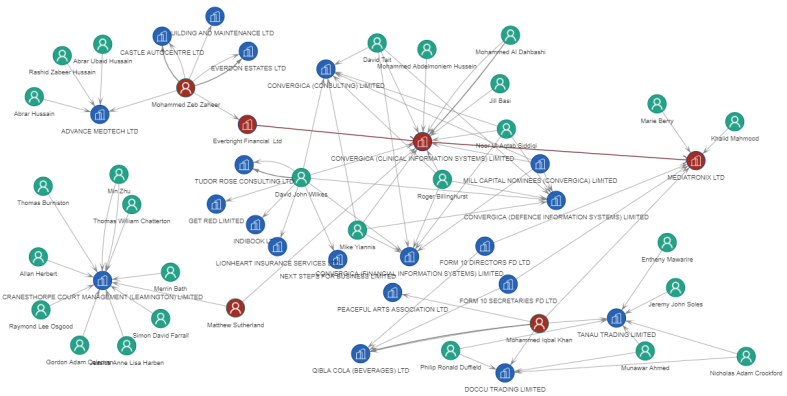
Matthew Cox, American author and ex-con artist, specialised in synthetic identity

Focus: R&D tax relief fraud

Corona brings new tax frauds

The coronavirus pandemic triggered the competition between different countries for supremacy in the digital world.

The United Kingdom decided to support its domestic tech industry with tax relief for capital expenditure on research and development projects. Scammers defrauding this tax framework have already made their first illicit profits. Matthew Sutherland, Mohammed Zeb Zaheer and Mohammed Iqbal Khan organised a fraudulent scheme that extracted almost 30 million pounds in fraudulent tax relief. The tax relief was claimed through Convergia LTD (Clinical Information Systems). The company controlled by Sutherland (he was not officially its director) subcontracted development work for 137 million pounds to Mediatronix LTD, where Mohammed Iqbal Khan served as director. The funds were loaned to Convergia by Everbright Financial LTD a company controlled by Mohammed Zeb Zaheer. Everbright does not appear in the British company registrar. Based on these expenses, Covergia was able to deduct 230% of the research expenses, thereby generating a loss for the British taxpayers.



Case Study: Convergica

The word on the street: New indictments in Philadelphia

Acting capo in jail

Last week, the FBI hit the Philadelphia based faction of “La Cosa Nostra” with a set of indictments. Fifteen alleged mobsters of the Philly family are facing racketeering, extortion, gambling and drug

trafficking charges. Amongst them, the federal agents brought in Steven Mazzone, the alleged leader of the group.
The Philadelphia family had a tormented past after going through a bloody war in the early 1990s. Throughout the 2000s the family was under the leadership of Joseph Ligambi, which put things in order and kept the activity under the radar, avoiding free media publicity like in the Scarfo-Merlino era. After Ligambi caught a few charges, Mazzone got the power and became the acting street boss. With this new indictment, the family may go through further restructuring.

Know Your Network, AI meets KYC

More insights at schwarzthal.tech

Marius Frunza
marius.frunza@schwarzthal.com

The information and data published in this newsletter were prepared by the market research department of Wunderschild.

Contact

contact@schwarzthal.com
FR: (33) 6 27 29 78 34
UK: (44) 7 95 22 08 734
RU: (44) 7 95 22 08 723

Address

231B Business Design Center London, N1 0QH, United Kingdom

Social

twitter.com/schwarzthal

linkedin.com/company/schwarzthal-tech