FinCrime & technology in the future

Financial economic crime (FEC for short) takes many different forms; from money laundering and terrorist financing to trade in illegal substances and evading tax using cryptocurrency. We interviewed several financial crime, cybercrime, cryptocurrency and OSINT experts to get the most complete picture possible of current and future trends in Financial economic crime. We discussed the variety of criminal activities, the contemporary challenges faced by analysts and investigators, and how technology can support the fight against FEC now and in the future. In this whitepaper, you can read all about our findings from these interviews.

DataExpert

What are the developments surrounding FEC?

A few years ago, a few major money laundering cases and scandals came to light at several major Dutch banks. At the time, significant fines were issued by De Nederlandsche Bank (DNB) to the banks concerned. Since then, the DNB has been strictly monitoring whether these banks comply with their gatekeeper role, which is to ensure that customers are properly screened upon admission. This phenomenon is known as the Know Your Customer (KYC) principle. It is also checked whether transactions are indeed actively monitored for possible money laundering and corruption. These activities fall under the Prevention of Money Laundering and Terrorist Financing Act (Wwft). Consequently, in recent years, major banks have hired thousands of analysts who deal with KYC and transaction monitoring on a daily basis.

In addition to governments and banks that have begun to monitor financial economic crime more closely, the public has also become more aware of the phenomenon. This is partly due to the leaks of the Panama and Paradise papers, but other well-known cases, such as the billion-dollar fraud at Wirecard, have also attracted public interest. As a result, public pressure to combat money laundering, fraud and corruption has increased significantly.

Tighter supervision from banks and society, and strict laws and regulations have made it necessary for criminals to look for other, creative and more anonymous forms of crime to make money. And one might argue that they found them. Below, we highlight some current forms of FEC that came up during the expert interviews.

Figure 1: Example of Wirecard fraud c

Cybercrime

Cybercrime has exploded in recent years. It is no longer a schoolboy hacking someone in the attic, but fully organised companies carrying out criminal practices. Cybercrime offers criminals not only the opportunity to scam financial institutions or attack large companies, but there has also been a sharp increase in victimisation among SMEs, for example. These companies often do not have enough resources to protect themselves optimally against things like Malware or Ransomware. Consumers are also a favourite target. They are easily scammed using social engineering techniques. Consider dating fraud (recent example, the Tinder Swindler), identity fraud and Phishing.
Besides attacking businesses and consumers directly, trading PayPal accounts, bank account numbers, credit card details or sensitive data on the darkweb is another form of cybercrime that takes place.

Cryptocurrency

Cryptocurrency and the blockchain offer interesting opportunities for trading and making payments. Besides trading via crypto wallets and using Decentralised Finance services, there are now also Bitcoin ATMs and crypto credit cards that provide many financial benefits. Cryptocurrencies owe their popularity in part to their anonymous nature. Through decentralised platforms, individuals can directly access various financial services without having to identify themselves. The anonymous nature makes the world of cryptocurrency extremely interesting for criminals. Criminals regularly use cryptocurrency to launder money, demand ransoms and evade taxes.

Example of tax evasion with NFTs (Non Fungible Tokens):

Person A possesses a Bored Ape NFT as shown in the image below. This ape with rainbow cap is worth 110 Ethereum. The NFT is registered with Binance, a centralised exchange. Because centralised exchanges require verification of users' identity (including ID card/passport), the assets of individuals on these exchanges are traceable by the tax authorities. To avoid tax, Person A can "sell" the ape to a proprietary decentralised wallet such as MetaMask for just a fraction of its actual value, as an example we will take 0.2 Ethereum. The tax authorities can then only see the 0.2 Ethereum as assets and cannot verify to whom the NFT with an actual value of 110 Ethereum was sold.

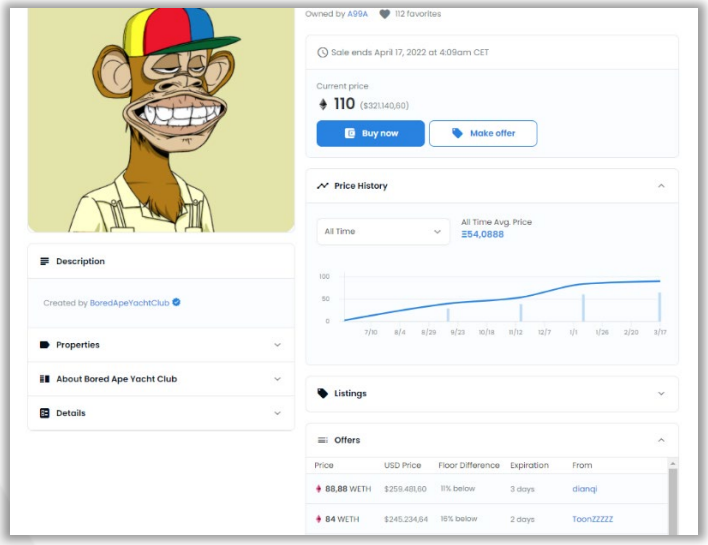

Figure 2: Bored Ape NFT (source: opensea.io)

Scamming through FinTechs

FinTechs have a growing role in the financial sector. FinTech is a compound of two words: financial and technology. FinTech companies combine financial services and products with innovative technology. Examples of successful Dutch FinTechs include Knab & Bunq (FinTech banks) and Adyen & Mollie (Payment Service Providers).

Because the DNB wants to allow sufficient room for innovation in the financial market (source: dnb), they are not as stringent in their monitoring of e.g. onboarding processes and transaction monitoring measures at start-up FinTechs. In addition, it is not easy for the DNB to adapt regulations to the rapid technological developments in the financial market in time. This makes it quite easy for criminals to use the FinTechs' financial services. They often only need to take a photo, scan an ID card and fill in some contact details. Once approved, they can not only use the services of FinTech, but also do things like using derivative identification to request credit cards from other financial service providers for malpractices.

Trade-based money laundering

In addition to financial economic crime in the digital world, fraud continues to be committed in the physical world. One of these forms of fraud is trade-based money laundering (TBML). This involves criminals setting up trading structures to launder money. These are often well-organised structures. A good example of TBML is money laundering through export of potatoes. Criminals invest cash in commodities that are then exported to and sold abroad. The identification of TMBL now often happens by chance, but it is estimated that millions are laundered (source: AMLC)

What are the expected new forms of FEC?

According to all experts interviewed, besides the examples mentioned above, it is impossible to predict which forms of financial economic crime will occur in the future. (Cyber)criminals remain flexible and regularly change their ***modus operandi***. Perhaps criminals will switch back to traditional payment methods where they will again use paper forms to transfer money and cash, while detection is mainly digital.

What did emerge from the interviews is the expectation that crime tracking will become increasingly complex. In the cryptocurrency world, for instance, work is already in full swing to build so-called mixers for different blockchain technologies. A mixer is a kind of blender that shreds multiple transferred digital currencies into pieces and then spreads them across multiple transactions. With this development, the Follow the Money principle might just be made impossible with regard to money laundering detection in the cryptocurrency world. The image below from the Dutch Tax Authorities is a good illustration of the mixer principle.

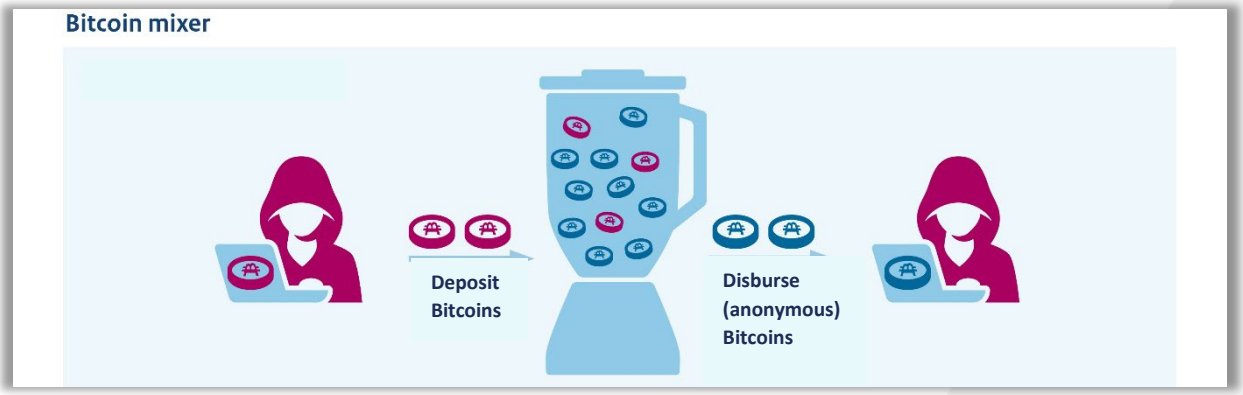

Figure 3: Bitcoin mixer (source: FIOD)

What are the challenges involved in detecting FEC?

Keeping knowledge up to date, intensifying international cooperation and large amounts of complex data combined with too little time.

Keeping knowledge up to date

One of the biggest challenges according to the experts interviewed is keeping the knowledge of investigators and analysts current and up to date. Only by understanding what steps criminals take and having a lot of domain knowledge can crime be successfully detected. This is because criminals are constantly refining their modus operandi and adapting their modus operandi based on new technologies and laws and regulations.

International cooperation

Because there are many different means of payment and different forms of crime, interview respondents said there is a need for cooperation at international and national levels, as well as within companies. For example, it would be desirable to have a single central organisation to handle customer onboarding for banks. As a result, each bank would not have to onboard each customer themselves, saving a lot of time and resources. Unfortunately, working together is easier said than done. The laws and regulations, including GDPR (General Data Protection Regulation), make this very difficult and even impossible in many cases.

Too much complex data and too little time

Another challenge that emerged in every conversation was the large amount of data involved in investigations. Investigators and analysts are faced with many different data sources and data formats: open sources, transaction histories, customer-supplied documents, et cetera. Worse yet, this data is often spread across dozens of systems. Despite the availability of technology, it still requires a lot of manual work and a huge amount of manpower, and therefore money, to sift through all this data and identify relevant information in a timely manner. The wide variety of case histories also makes it difficult to standardise processes.

Keeping risk indicators up to date

Currently, standard lists and indicators are widely used within financial institutions and in the investigation world. But what if a new phenomenon emerges? Will it be detected? Also, people now often look at outliers (anomalies), but in forms of crime such as trade-based money laundering, there are no such outliers. It is therefore important to continuously update the risk indicators used.

Which technologies can support analysts and investigators in the fight against FEC and why?

The basis for successful crime fighting is the knowledge and experience of analysts. However, technology can be of great help to investigators and analysts in exploring data, understanding data, analysing data and then turning data into actionable intelligence. Below, we highlight several technologies from the DataExpert portfolio that can simplify the fight against financial economic crime.

Collecting data from open sources

Data from open sources can enrich your own data and can help with customer onboarding (KYC) and network mapping. There are many different platforms, products and plug-ins on the market that can help search, collect, monitor, analyse and report on data from open sources.

One very popular open source intelligence (OSINT) tool within the investigation world is **Maltego**. **Maltego** allows investigators and analysts to collect and connect information from open sources such as the darkweb, forums and Reddit. The software features a graphical link analysis interface and many transforms that allow the integration of other tooling into the platform through API access.

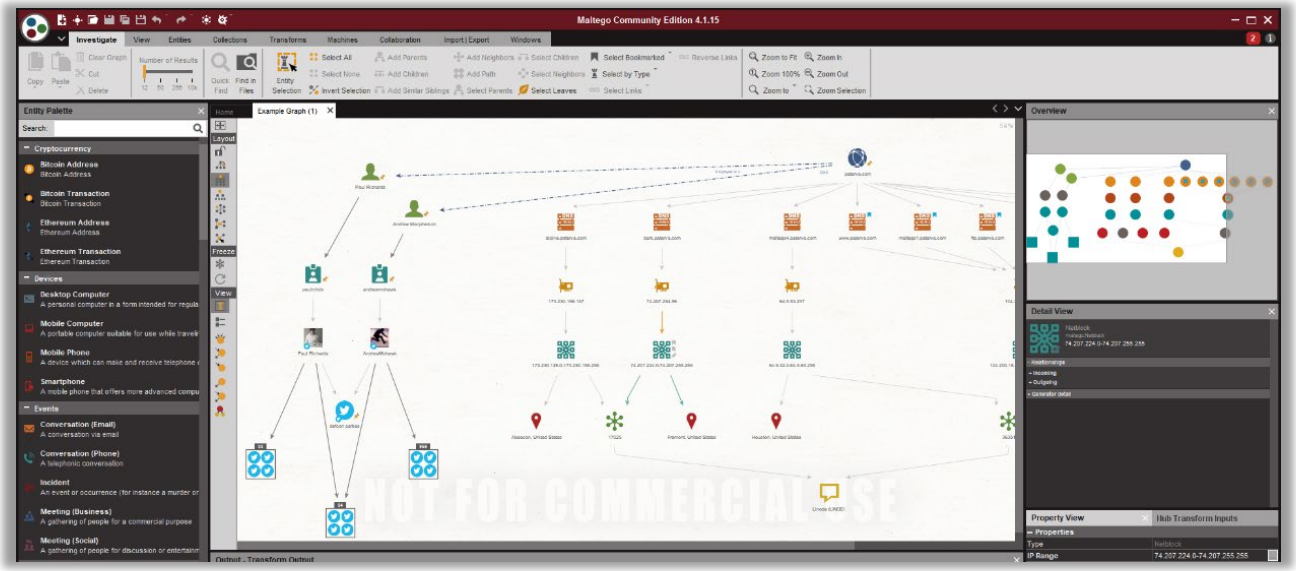

Figure 4: Maltego software

There are also Web Intelligence platforms such as **Cobwebs** that extract targeted intelligence from large amounts of data using machine learning algorithms. For example, Cobwebs helps investigators and analysts with (real-time) monitoring of online activities and collecting and analysing data from digital open sources, social media and the deep and dark web.

Extracting & analysing unstructured data

More and more data used for the purpose of crime fighting is unstructured; e.g. content from news reports or social media posts. The lack of a single standard structure, the volume of data available (big data) and the many formats complicates the analysis process. The software solution **i2 TextChart** allows analysts and investigators to extract from many thousands of e-mails, public sources and/or financial documents, locations and other entities and relationships for further visualisation and analysis. i2 TextChart enriches the visualisation and network analysis of structured data with automated extractions of more than 36 different types of entities, 200+ relationships and (geographical) locations.

Figure 5: i2 TextChart

Financial Crime Analysis

Software such as **i2 Analyst's Notebook (Premium)** helps investigators and analysts make sense of data through search and link analysis functionalities. Various types of structured data (telephone conversations, transactions, IP addresses, etc.) are compared and visualised through heatmaps, relationships, histograms and diagrams, etc. Relational networks, timelines and geographical overviews thus become clear at a glance. Using the visualisation functionalities, investigators and analysts can then visualise the modus operandi of criminals.

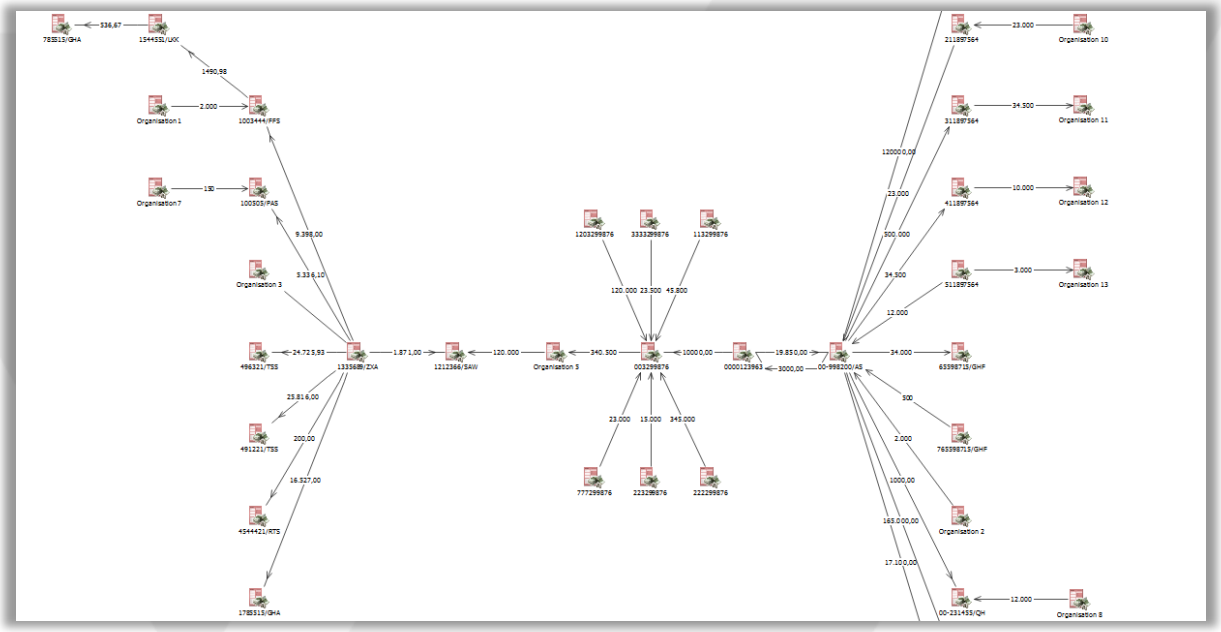

Figure 6: i2 Analyst's Notebook

Analysing cryptocurrency transactions

As described earlier, cryptocurrency is favoured by many criminals. And while they make it handsomely difficult for investigators and analysts to monitor their transactions, it is not impossible. After all, cryptocurrency transactions are stored in a public ledger. Using advanced technology, cryptocurrency transactions in the blockchain can be monitored, collected and analysed in order to generate the right insights to combat money laundering and terrorist financing. **Chainalysis** offers various solutions for conducting cryptocurrency investigations.

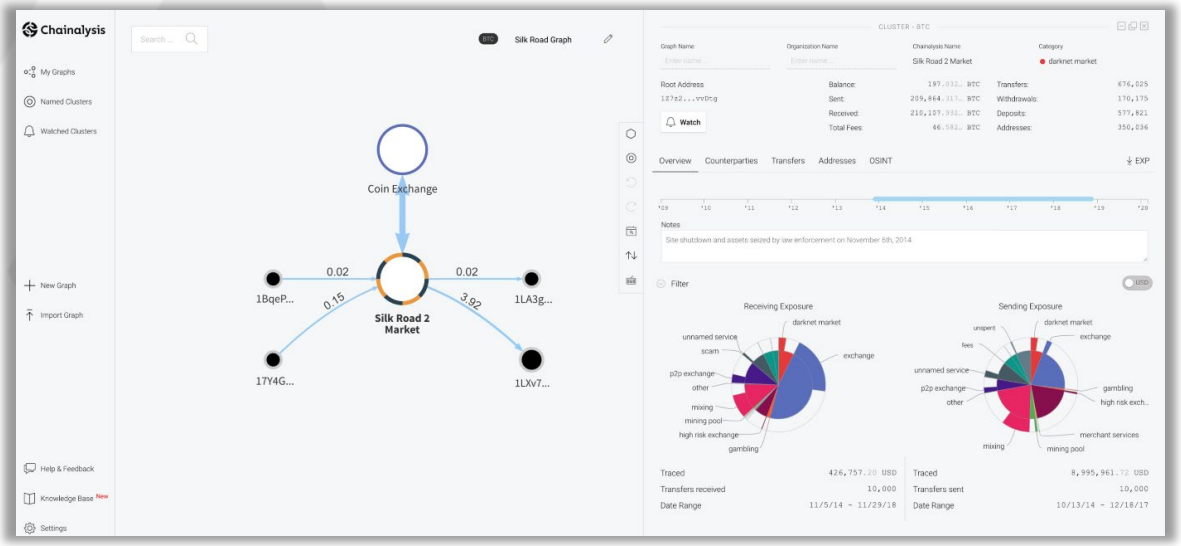

Figure 7: Chainalysis

What does the technology of the future look like?

As described above, there are many different tools in the market that can support analysts and investigators in their investigations. Despite the already broad range of options, we were also curious to know what could be improved in terms of technology in the future. Interview respondents came up with one clear desire: **a platform where all data sources can be searched simultaneously in a Google-like manner.** Ideally, it should also be a scalable solution and not involve expensive hardware costs.

The experts also said they expect AI/Machine Learning to unburden analysts and investigators in the future by automatically scanning huge data sets, identifying patterns and anomalies, making connections and summarising results. In fact, the first steps toward this have already been taken. For example, the tool Cobwebs described above already uses AI.

Conclusion

After all the interviews, one thing has become clear to us: **we can't sit on our hands!** To keep up with the developments within financial economic crime, it is important that investigators and analysts (continue to) have the right skills and expertise. In short: train, train, train and share knowledge.

The right technology can also help financial institutions and investigators understand the complex modus operandi of criminals. By efficiently collecting, aggregating and analysing data, networks can be mapped, timelines made clear and anomalies filtered out.

DataExpert is at your service

Which methods and tools in the fight against financial crime are appropriate within an organisation varies. This depends on the type of data sources being worked with, the capacity, the desired investigations, the budget, etc. The experts at DataExpert are happy to help you identify the right method for you.

We can also train you and your colleagues in analysing (cryptocurrency) data with and without tools, conducting OSINT investigations and visualising cybercrime.

Dutch office

P: +31 (0)318 543173
E: info@dataexpert.nl
W: www.dataexpert.eu
A: Vendelier 65, 3905 PD Veenendaal

Swedish office

P: +46 735 000644
E: info@dataexpert-se.se
W: www.dataexpert-se.se
A: Storgatan 32A, SE-582 23 Linköping

Danish office

P: +45 5350 6959
E: info@dataexpert.dk
W: www.dataexpert.dk
A: Mølledammen 24, 3550 Slangerup