

# ACUMINOR

Going dark and getting rich

Criminal misuse of virtual currencies



## **In March 2018 the CEO of the Canadian company Phantom Secure was arrested.**

Phantom Secure provided secure cell phones that were purposely built to avoid law enforcement, facilitating the transnational smuggling and large-scale distribution of narcotics. Many of Phantom Secure's clients were vendors of illegal goods and services on the darknet and serious crime organisations like the Sinaloa cartel. The phone subscription plan ranged from \$2000 - \$3000 per six months and over 20 000 phones were sold. Phantom Secure assets worth tens of millions of US dollars were eventually confiscated, ranging from bank account assets worldwide, to houses, a Lamborghini, virtual currency accounts and gold coins.

A major reason to why Phantom Secure was able to avoid law enforcement detection for an extended period of time was the use of virtual currencies. The virtual currencies served to protect the anonymity of Phantom Secure's clients and launder proceeds deriving from the serious drug offences that they took part in.

*"The virtual currencies served to protect the anonymity of Phantom Secure's clients"*

## **The Good, the Bad and the Ugly**

The Phantom Secure case illustrates how the development of the financial landscape has not only given us new opportunities, but also quite a few challenges. It's pretty easy nowadays to initiate payments from a third party, connect multiple payment options in a single transaction while relying on a remote customer relationship (while taking advantage of a somewhat unclear division of responsibilities between service providers). This means that it's also pretty easy to make payments that goes dark and flies below the radar of financial institutions and, in extension, law enforcement.

## **A case amongst many**

Obviously, the Phantom Secure is not unique. Europol has raised the issue that organised crime groups involved in corruption is increasingly misusing online services. Some criminals use virtual currencies and alternative payment platforms to transfer funds to their accomplices in the public and private sector.

Criminal misuse of virtual currencies has been identified in cases of for example:

- Corruption
- Drug trafficking
- Drug smuggling
- Terrorist financing
- Sanction violations (Iran and Russia)
- Human trafficking
- Arms trafficking

## **Could a financial institution detect criminal misuse of virtual currencies?**

Eventually, virtual currencies must be exchanged into local FIAT currencies in order to enable purchases of houses, cars or other necessities. Generally speaking, it is only at this stage that a financial institution could potentially detect that something is going on.

There are numerous different methods for the exchange, and they are constantly evolving. At the moment there is a trend to use peer-to-peer transfers and alternative payment platforms to facilitate such activities.

### **Peer-to-peer exchanging**

Peer-to-peer exchanging is an exchange between private individuals. Person "A", the bitcoin holder interacts with Person "B", the FIAT currency holder who is acting as a virtual currency exchanger. "A" initiates a bitcoin wallet-to-wallet transaction to person "B". Person "B" sends FIAT currency at an agreed upon exchange rate to:

- a bank account
- a mobile payment platform
- a prepaid card

*"The battle is not completely lost"*

## **Alternative digital banking platforms**

There are a multitude of payment platforms with specific product offerings, for example: Electronic wallets where individuals can store and convert virtual currencies and deal directly with FIAT options within the same platform. You can for example can fund an account with:

- A private virtual currency wallet
- Credit/debit card
- Bank account
- Peer-to-peer transfers between users within the same platform

The digital banking platform provider is often acting as a card issuer, so individuals can withdraw funds in FIAT currency directly through a connect payment card.

### **The battle is not completely lost**

As explained above, the increase of new business models that enables money flows between virtual currencies and FIAT products gives new possibilities to engage in legitimate transactions, but also creates transportation channels for illicit money. Virtual currencies connected to crime is primarily used to transact between different parties and is not used for long time storage of criminal proceeds.

In the case of Phantom Secure, virtual currencies turned out to be an ideal means of payment in order to limit the financial trail where financial institutions or law enforcement agencies could connect the dots. Could the financial institutions where Phantom Secure and its culprits were banking have detected that a large-scale criminal operation was going on? Definitely not based on the virtual currency transactions as such. But maybe when the exchange into cold hard money was made. ■

## **Terms of use**

You are free to use this report for your own personal development, in internal training or in other risk management activities.

You are of course not allowed to resell this report, nor claim that you have made it yourself.

*Please remember to state the source as follows: Acuminor (2018). Go dark and get rich - Criminal misuse of virtual currencies. Report 2018:3. Stockholm: Acuminor.*