SymphonyAI
SENSA-NETREVEAL

BANKING INSIGHTS

When does cyber crime become FinCrime?

And what are the consequences?

Introduction

Cyber crime is an all-encapsulating term, covering digital or internet-based intrusion and action. Corporations and institutions are well versed in putting into place security practises and safeguards to help protect their organisations and their customers and products. Nonetheless, cyber crime as a mechanism to commit financial crime (FinCrime) has escalated in the last decade as the digital age has taken hold.

The complex interplay between cyber crime and FinCrime is becoming more visible, with countries such as the UK raising cyber crime's profile in the economic crime plan,[1] and with European anti-money laundering (AML) regulations articulating cyber crime as a predicate offence.[2]

As digitisation efforts continue (indeed the Covid-19 pandemic accelerated many of these), and as threat actors become more sophisticated and specialised in their crime craft and/or money laundering capabilities, the overlap between cyber crime and FinCrime is one that cannot be ignored and must remain a priority among financial institutions.[3] [4]

In this banking insights paper, Taylor Humphreys, FinCrime threat intelligence analyst at SymphonyAI Sensa-NetReveal, **explores the challenges faced by financial investigators in banks** as they tackle cyber crime in relation to money laundering.

Why are we talking about this?

SymphonyAI Sensa-NetReveal is dedicated to helping financial institutions better detect criminality. Key to this is equipping them with an understanding of criminal trends and behaviours so that our customers can try to stay ahead of threat actors.

The FinCrime testing service (FTS) is an anti-money laundering (AML) product focusing on helping to improve the abilities of financial institutions to identify criminal typologies in financial data. The FTS tests the effectiveness of bank's AML systems using data to simulate criminal behaviours, with the aim to reduce the risk that the bank might unwittingly help launder the proceeds of cyber crime.

For this, the FTS team are constantly researching actor and victim profiles, and the methodologies and techniques commonly used by threat actors to develop solutions which most closely resemble real-world criminality. In turn, this will help improve the volume and accuracy of crime detection.

Click here to find out more about our FinCrime testing service

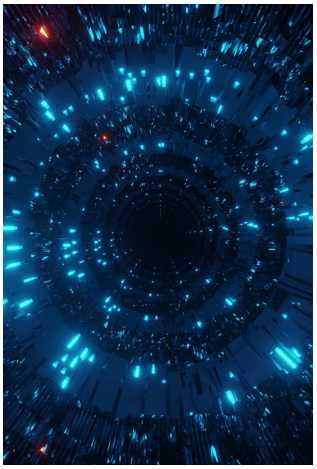
The cyber crime/FinCrime overlap

Traditional distinctions between cyber crime and FinCrime are blurring.[5] If a cyber criminal has a financial motivation, there will be an overlap between cyber crime and FinCrime, because the illicit proceeds will need to enter and move through the financial system for criminals to benefit monetarily from the cyber intrusion element of the crime.

This interplay is far more complex in reality. Agile threat actors are constantly adapting, resulting in a race between threat actors on the one hand, and regulators, law enforcement and financial institutions on the other. As cyber criminals develop more lucrative attacks, the opposing side must, in response, race to increase protection, detection and disruption efforts. An issue which has only been exacerbated by the Covid-19 pandemic, as we have seen a sudden switch to remote working and socialising, with cyber hygiene following slowly behind. This has afforded cyber criminals a greater pool of potential targets and opportunities for compromise.[6]

Financial institutions face increased responsibility

Financial institutions are at risk of being directly targeted by cyber criminals, with 'cyber heists' or business email compromise (BEC) attacks being examples of known and recent methods. For example, North Korean state-sponsored threat actors stole $81 million from the Bank of Bangladesh in a cyber -heist in 2016, and a more recent case in 2019 saw the attempted theft of approximately €13 million from the Bank of Valletta. [7] [8]



However, financial institutions also risk facilitating the monetisation of cyber crime in relation to AML failures because they are directly exposed to the process.

In working to better understand cyber crime as a predicate offence to money laundering, financial institutions will be in a better position to detect and report suspicious activity perceived to be in relation to cyber crime. This will help to enhance the quality and accuracy of suspicious activity reporting, better equip law enforcement to investigate cyber crime, help protect financial institutions from the potential repercussions of inadequate AML efforts, and help in the whole-of-society approach to tackle cyber crime.

Regulations

- In light of the above, regulators have placed increased responsibility on financial institutions in relation to cyber crime and AML. Numerous regulatory bodies across the globe have been talking about cyber crime, FinCrime, and money laundering for a number of years, including the financial crime enforcement network (FinCEN) in the US, the financial conduct authority (FCA) in the UK, and the Australian transaction reports and analysis centre (AUSTRAC) in Australia, to name a few. [9] [10] [11]
- Significantly, cyber crime was explicitly recognised as a predicate offence to money laundering for the first time in the European Union's 6th AML Directive, published July 2021.[12] The Directive defined 22 predicate money laundering offences in an effort to harmonise the understanding of money laundering across the EU. For banks to be compliant with the new Directive, they must be aware of the predicate offences, know how to identify them, and how to act upon suspected suspicious activity.[13] As noted, cyber crime is one of the newly defined predicate offences. These regulations increasingly call for institutions to understand the various threats posed by cyber crime, and how to better detect and report indicators of cyber criminality.
- While the EU directive is for EU member states and those that choose to follow their rules, as noted previously, cyber crime has been on the EU regulator's agenda for a number of years, and it can be reasonably suggested that in the near future, other regulators may also recognise cyber crime as predicate offence to money laundering and alter their regulations accordingly.

Key insight

To assist in this area, SymphonyAI Sensa-NetReveal is investigating the money flow of different types of cyber crime and simulating the associated behaviours. The simulated behaviours will be based on intelligence from law enforcement, open-sources and subject matter experts to produce a simulation which most closely resembles real-world criminal and victim profiles to test the effectiveness of bank's AML systems.

Categorising cyber crime by laundering methods

We have defined and outlined different types of cyber crime in terms of their cyber intrusion element, detailing typical techniques, tactics and procedures (TTPs). They have then been categorised by the methods perpetrators typically use to cash out/monetise illicit funds.

These categories reflect the fact that many different types of cyber crime behave similarly financially, despite having entirely different intrusion processes. So, from the financial indicators alone, it is often impossible to accurately guess which type of crime the funds originated from.

For example, although the cyber-intrusion elements of BEC and banking Trojan attacks are entirely different, when attempting to monetise illicit proceeds, both types of cyber crime can involve the use of the attacker's own bank account, or of an unknowing money mule's bank account. Therefore, the purpose of grouping different types of cyber crime together is to come as close as possible to applying accurate money laundering methods to specific types of cyber crime.

As such, the defined types of cyber crime have been grouped into the following categories:

01. Illicit funds move from the victim's bank account to cryptocurrency

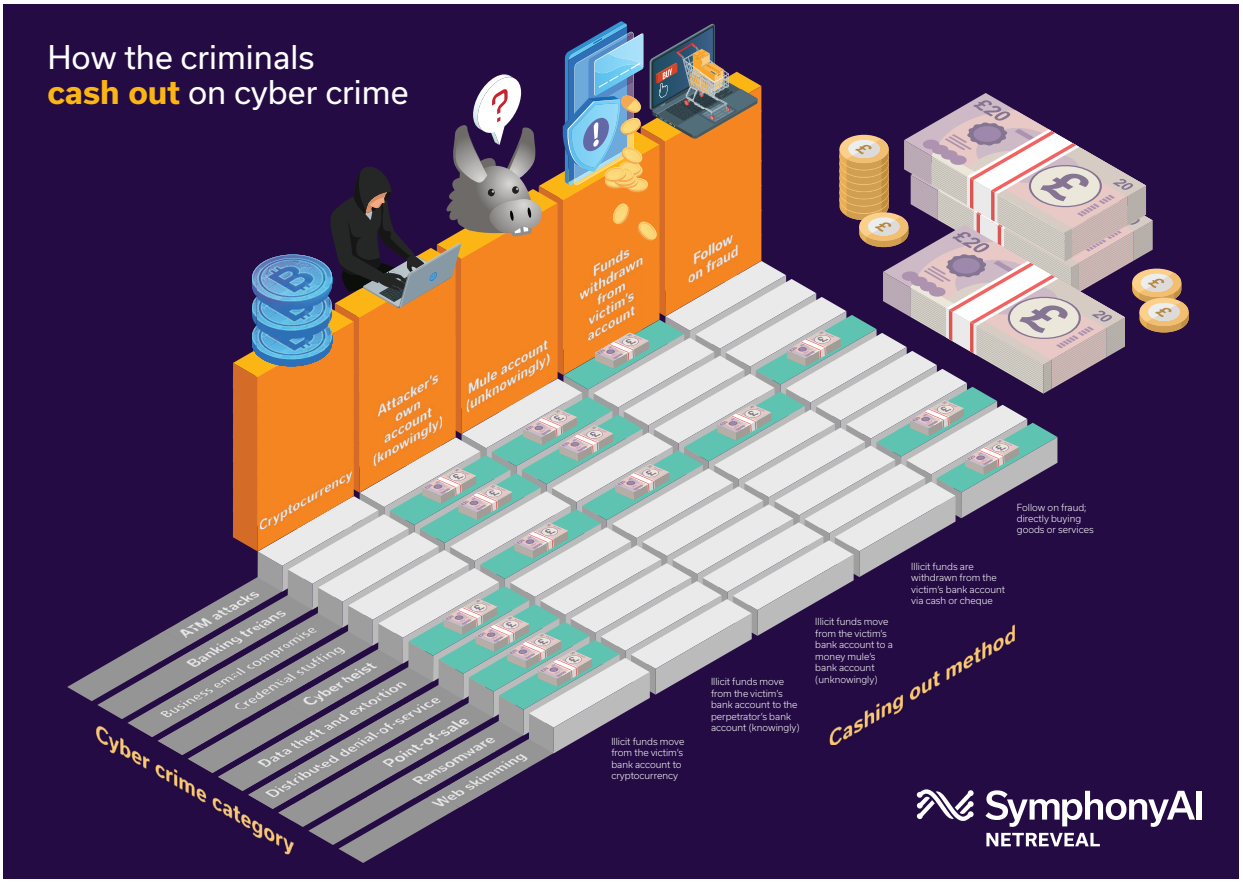
02. Illicit funds move from the victim's bank account to the perpetrator's bank account (knowingly)

03. Illicit funds move from the victim's bank account to a money mule's bank account (unknowingly)

04. Illicit funds are withdrawn from the victim's bank account via cash or cheque

05. Follow on fraud; directly buying goods or services

It must also be noted that one type of cyber crime may fit into multiple monetisation categories. This reflects the idea that crime is not a linear concept, and not all criminals will think and behave alike, as criminals can adopt many different methodologies but still arrive at the same end result.



Application to specific typologies

From an automated detection point of view, these general categories really help, however, when investigating suspicious alerts, an even more nuanced understanding is required. Therefore, we will now work through two real life examples that really bring the cybercrime categorisations to life.

Example 1: Hushpuppi

The first case study explores the illicit actions of money launderer and international mule organiser, Ramon Abbas. Known to his 2.5 million Instagram followers as 'Hushpuppi', Abbas engaged in a series of sophisticated internet scams, cyber-heists, and BEC attacks to steal an estimated total of $24 million from his victims throughout 2019.[14] As a result, Hushpuppi was arrested for his crimes at his home in the Palazzo Versace Apartments, Dubai in June 2020.[15]

In tracking the precise movement of funds and developing an understanding of the money flow and laundering processes employed by Abbas and his affiliates, significant findings regarding the type of bank accounts favoured, the range of laundering techniques employed, and the interconnectivity between players across the cyber crime and money laundering spheres have been uncovered.

Example 2: Ransomware

In exploring how ransomware payments typically enter and move through the financial system, and identifying the process by which attackers come to benefit financially from ransomware, financial institutions will be better equipped to spot ransomware payments moving through their systems.

Particularly, in investigating the ransomware payment and proceeding money laundering methods typically employed by threat actors, a series of key indictors specifically relevant for financial institutions have been identified. These indicators will form the basis of the FTS's simulation of a ransomware payment. This simulation will be used to test the effectiveness of financial institutions abilities to detect their customers paying a ransomware demand.

Final thoughts

Ultimately, in categorising different types of cyber crime, mapping their associated money flows, and coming to understand the typical ways in which threat actors launder cyber crime proceeds, it becomes possible for financial institutions to identify potential indicators of suspicious activity.

The FTS team's aim is to continue researching different types of cyber crime in greater detail, and to apply the relative categorisations to generate an even greater understanding of criminality.

In feeding this kind of information into the simulation of additional cyber and traditional criminal typologies, we are developing a comprehensive library of criminal behaviours which will be able to further enhance financial institutions' detection, reporting and compliance initiatives, for a wide range of typologies.

Click here to find out more about our FinCrime testing service

Taylor Humphreys, FinCrime threat intelligence analyst, SymphonyAI Sensa-NetReveal

Taylor is a Fincrime threat intelligence analyst at SymphonyAI Sensa-NetReveal, working across the cyber threat intelligence team and the FTS team with four years of academic study dedicated directly to the fields of crime, security, and intelligence.

Motivated to assist the financial sector in using data to better detect criminality, Taylor researches and articulates different types of cyber criminal behaviours to be used to test the effectiveness of financial institution's AML solutions. To do this, Taylor triages intelligence from law enforcement, subject matter experts, financial institutions, open-sources and regulators, to provide an articulation of cyber criminality that most closely resembles real-world criminal behaviours.

About SymphonyAI Sensa-NetReveal

SymphonyAI Sensa-NetReveal, a division of SymphonyAI, provides leading AI-based financial crime detection software. Learn more at netreveal.ai.

Contact us for more information:
netreveal.ai/contact

[1] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022
[2] https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en
[3] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyber attacks-during-COVID-19
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423
[5] https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/transforming-approaches-to-aml-and-financial-crime
[6] https://www.forbes.com/sites/adigaskell/2022/03/02/the-cyber security-challenges-of-working-from-anywhere/?sh=5ac649be14cc
[7] https://www.bbc.co.uk/news/stories-57520169
[8] https://www.zdnet.com/article/three-suspects-arrested-in-maltese-bank-cyber -heist/
[9] https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cyber crime%20508%20FINAL.pdf
[10] https://www.fca.org.uk/publication/research/future-horizons-conference-cyber crime-paper.pdf
[11] https://www.austrac.gov.au/serious-financial-crime-taskforce-tackles-cyber crime-offshore-tax-evasion-and-illegal-phoenix-activity
[12] https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en
[13] Ibid
[14] https://www.bbc.co.uk/news/world-africa-58002932
[15] https://www.researchgate.net/profile/TaiwoOlaiya/publication/343529810_Narrative_of_Illicit_Money_'Yahoo'_Boy_Format_of_Cyber _Scams_and_Governance_Challenges_in_Africa/links/5f2ebbb0458515b7290e9714/Narrative-of-Illicit-Money-Yahoo-Boy-Format-of-Cyber-Scams-and-Governance-Challenges-in-Africa.pdf