MAFUNGO ATTORNEYS: FINTECH ARENA

JUNE 2022

CYBERCRIMES ACT 19 OF 2020

FINTECH: INVESTIGATION AND PROSECUTION OF CYBERCRIMES UNDER THE CYBERCRIMES ACT 19 OF 2020

- By Kalipa Mafungo

The President of South Africa proclaimed the commencement date of certain sections of the Cybercrimes Act No 19 of 2020 ("CCA") to commence on the 1st of December 2021[1]. The CCA seeks to further regulate aspects of jurisdiction in respect of cybercrimes, the powers to investigate cybercrimes; and, to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes[2]. Critical aspects in procuring convictions for criminal offences are concerned with the ability to detect offences, the ability (and will) to report offences, the ability to gather the evidence necessary to establish

[1] https://cybercrimesact.co.za/
[2] See the Preamble to the CCA

the commission of the offences detected and the methodology employed in the gathering of such evidence inclusive of search and seizure protocols.

The CCA establishes various statutory cybercrime offences including cyber fraud, cyber forgery and uttering, cyber extortion and theft of incorporeal property[3]coupled with standard operating procedures to be adopted in relation to the investigation of such offences[4]. Fintech environments are, as the name suggests, rooted in technology providing fertile ground for hackers, scammers, extortionists and fraudsters who may deceive and prey upon financial services consumers in any number of ways including data theft, phishing schemes, extortive practices or the unlawful acquisition or use of passwords or access codes to a device (also an offence under the CCA). Financial services are regulated by the Financial Sector Conduct Authority ("FSCA") creating an element of intersectionality between the prosecution of cybercrime by the National Prosecuting Authority ("NPA"), its investigation by the South African Police Service ("SAPS") and its detection by the FSCA.

A framework of co - operation between organs of state has been provided for in the Constitution[5] which dictates that the NPA, SAPS and the FSCA[6] must co -operate with one another in good faith by:

- Assisting and supporting one another;
- Informing one another and consulting on matters of common interest;
- Co-ordinating their actions and legislation with one another; and,
- Adhering to agreed procedures.

Fundamentally, criminal activity involving cybercrime takes place through the use of digital or electronic devices on digital platforms. In 2021 cryptocurrency crime accounted for 14 billion dollars[7], with South Africa taking its fair share of damage with 3.6 billion dollars being fleeced from consumers, allegedly by Raees and Ameer Cajee who operated the Africrypt platform[8]. The parties involved in these schemes often use the latest innovations and technology[9]. Could the Africrypt scandal have been avoided if the prevailing regulatory and supervisory regime was equipped with the necessary tools to avoid such an outcome? or if the eventuality materialized, could the culprits be swiftly held accountable on the strength of evidence collected through analytics extracted from the digital platforms employed to transact on the Africrypt platform? Most probably yes. Regulatory Technology ("RegTech")[10]and Supervisory Technology ("SupTech")[11]provide for avenues to address this. According to the Intergovernmental Fintech Working Group ("IFWG"), globally, financial crime surveillance accounted for 46% of SupTech and RegTech activity, with data management accounting for 6%, eKYC/AML/CFT 12%, Risk Management 12%, Regulatory Reporting 3% and Regulatory Compliance Support 21%[12].The objects of SAPS include the prevention, combatting and investigation of crime[13]. Where cryptocurrency

[3] Sections 8, 9,10 and 12 of the CCA
[4] Section 26 of the CCA
[5] Section 41
[6] All being organs of state as defined in section 239 of the Constitution
[7] Article by Megan DeMatteo dated 16 May 2022 accessible at https://time.com/nextadvisor/investing/cryptocurrency/common-crypto-scams/
[8] https://www.coindesk.com/business/2022/01/11/south-african-police-investigate-missing-brothers-crypto-platform-africrypt/
[9] https://www.sec.gov/files/ia_virtualcurrencies.pdf
[10] Defined as the management of regulation, compliance, reporting and monitoring through technologies like big data, data mining, artificial intelligence and blockchain to provide robust, reliable and effective solutions by cointelegraph. See https://cointelegraph.com/explained/what-is-the-importance-of-blockchain-in-the-regtech-ecosystem
[11] Described as the use of innovative technology by supervisory agencies to support supervision by helping supervisory agencies digitise reporting and regulatory processes. See section 1 at page 3 of the Bank of International Settlements publication FSI Insights on Policy Implementation No 9 accessible at https://www.bis.org/fsi/publ/insights9.pdf
[12] See page 3 of Supervisory Technology document authored by Kagiso Mothibi and Awelani Rahulani accessible at https://www.fsca.co.za/Regulatory%20Frameworks/FinTechDocuments/Suptech%20in%20South%20Africa.pdf
[13] Section 205 (3) of the Constitution

exchanges and platforms do not qualify as financial services providers ("fsp's") subject to regulation under the FAIS regime or any other laws administered by the FSCA, they still fall within the scope of SAPS mandate to prevent, investigate and combat crime. Financial crime surveillance of cryptocurrency platforms would accordingly fall within the competency of SAPS *vis – a – vis* crypto platforms and individuals operating within South Africa's jurisdiction. Furthermore, pursuant to the establishment of the Directorate For Priority Crime Investigation ("DPCI" or more commonly known as "the Hawks")[14] within the SAPS; government departments and institutions are obliged to take reasonable steps in assisting the Hawks carry out their objectives, when required[15].

At a granular level the CCA prescribes Standard Operating Procedures ("SOP"s) directed at regulating the investigation, search and seizure of electronic evidence for the purpose of the prosecution of offences. It is at this stage that SupTech and RegTech could be most beneficial in the detection, prevention and general combatting of financial crimes carried out on or through the use of virtual platforms. It is not uncommon to see cops walking the beat or patrolling the streets of our cities and towns in marked vehicles alerting would be criminals to their presence, with the intention of averting crime. This is one of the measures employed by law enforcement to prevent crime. Of course, the actual presence of SAPS on our streets also places them in a position to react in real time should a crime be committed in the area that they are patrolling. What then is the appropriate equivalent to be employed by SAPS or the FSCA and other regulatory or supervisory bodies that oversee the activities of cryptocurrency service providers such as trading platforms that intermediate in the purchase and sale of cryptocurrency, issuers of cryptocurrency (initial coin offerings, stablecoins, tokens and utility coins and the like), digital wallet providers, virtual credit and financial service providers. How do SAPS and regulatory bodies walk the virtual beat to patrol the ecosystems in which these actors, their customers and would be cybercrime offenders operate? Unless it is suggested that for some reason these actors are entitled to operate beyond the field of vision of SAPS and regulators on platforms that engage the public; SupTech and RegTech provide the perfect (in principle) countervailing measures to check cybercrime and enforce the CCA within virtual ecosystems at a practical level.

The Financial Conduct Authority of the United Kingdom ("FCA") has embarked on an initiative to digitize regulatory reporting.to permit machine execution of reporting requirements that allows for regulations to be published digitally in code with the potential for the digital version of the regulations to be read alongside or accompanied by the natural language version of the regulation. Financial institutions may then be equipped to execute these regulations and forward reporting data to the authorities, with the authorities being possessed of a similar corresponding ability to extract reporting data from the financial institution[16]. Taken a step further embedded supervision[17] allows for the supervision of financial markets through the use of distributed ledger technology, distinct from SupTech and RegTech, by exploiting the trust (consensus) mechanism inherent in the notion of distributing and publishing every transaction contained in the ledger being supervised and making the authorities privy to such information [18]. The technology exists for SAPS, the FSCA and regulatory authorities within South Africa to consider similar options. The FSCA has issued various "crypto health warnings" to the South African public cautioning against

[14] Under section 17C of the South African Police Services Act No 68 of 1995
[15] Id at section 17F (1)
[16] Paragraph 34 of the Bank of International Settlements Financial Stability Institute publication FSI Insights on policy implementation No 29 December 2020 issue by Juan Carlos Cristano et al accessible at https://www.bis.org/fsi/publ/insights29.pdf
[17] a regulatory framework that provides for compliance with regulatory standards in DLT based markets to be automatically monitored by reading the market's ledger which is backed up by an effective legal system and supporting institutions. See the principles of embedded supervision at page 4 of the Bank of International Settlements Working Paper No 811 September 2019 issue revised for May 2022 by Raphael Auer accessible at https://www.bis.org/publ/work811.pdf
[18] Id at page 19

dealings in cryptocurrency[19] but has not taken active and concrete steps to tackle the dangers cautioned against in their health warnings. Would the cryptocurrency landscape not be that much safer and welcoming to members of the public dealing in good faith on virtual platforms knowing that these platforms have built-in checks against cybercrime and fraud coupled with financial crime surveillance? It would!

Decentralized Finance, blockchain technologies and associated virtual networks serve as the stage and provide the ecosystems within which many of the offences criminalized under the CCA take place. The South African Banking Risk Information Centre ("SABRIC") characterizes cybercrime as *"a socio-technical problem which is increasing at an alarming rate and will eventually replace many 'traditional' bank crimes as it transcends time and physical proximity due to its virtual nature. In addition, the convenience and anonymity of the internet make it easy for criminals to perpetrate these crimes. These digital attacks include unauthorized access to devices, identity theft and online bank information theft. Even more concerning, is its potential to infiltrate networks, resulting in mass data breaches"* [20]. The law is notoriously slow at keeping pace with technology with the result that cybercrime offenders often evade detection and prosecution whilst victims are left without remedy nor a face or person to whom they may attribute their anguish. For there to be any hope that the CCA will be effective in curtailing, combating and prosecuting cybercrime involving virtual currencies in South Africa, technology will have to be employed to keep pace with the innovations used by offenders in committing cybercrimes.

[19] https://www.fsca.co.za/TPNL/FSCA%20eNewsletter/fsca/regulatorycrypto.html ; fsca.co.za/News%20Documents/FSCA%20Press%20Release%20%20FSCA%20warns%20the%20public%20against%20BitCoin%20Xpress%2027%20August%202021.pdf

[20] https://www.sabric.co.za/stay-safe/cybercrime/