TECHNOLOGY &
COMMUNICATIONS SECTOR

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

THE CYBERCRIMES ACT: Cyber fraud and private sector reporting obligations

Compiled by Preeta Bhagattjee and Krevania Pillay

5 AUGUST 2021

The Cybercrimes Act 19 of 2020 (Cybercrimes Act) was enacted as a law on 26 May 2021, although the date that it will come into force is yet to be announced. Eleven new "*cybercrimes*" have been defined in terms of the Cybercrimes Act, including unlawful interception of data, unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices, cyber fraud and cyber extortion.

Focussing on cyber fraud, this cybercrime is defined as:

> *"8. Any person who unlawfully and with the intention to defraud makes a misrepresentation:*
>
> *(a) by means of data or a computer program; or*
>
> *(b) through any interference with data or a computer program as contemplated in section 5(2)(a), (b) or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(a),*
>
> *which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud."*

The definition of cyber fraud is strikingly similar to the common law definition of fraud, in which fraud is defined as "*the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another*". The difference, however, is that cyber fraud requires the fraud to be perpetrated with the intention to defraud but using a computer program or data or to be carried out through "*interference with data or a computer program*" or interference with a computer data storage medium or computer system. Any unlawful deletion or alteration of any data or computer program or obstructing, interfering with and interrupting of any lawful use of data or computer program also falls within the definition of a cyber fraud. Ransomware attacks, in which cybercriminals demand a ransom from individuals or entities to restore lawful control of IT infrastructure which they have unlawfully infiltrated, is an example of cyber fraud. Ransomware attacks also present elements which are congruent with the definition of cyber extortion, which extends to any person who unlawfully and intentionally commits or threatens to commit the cybercrime of:

- intercepting data, including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system (section3(1));
- interfering with data or a computer program (section 5(1));
- interfering with a computer data storage medium or a computer system (section 6(1)); or
- acquiring, possessing, providing to another person or using a password, an access code or similar data or device for purposes of contravening various provisions of the Act (section7(1)).

The above act(s) must be performed for the purpose of obtaining any advantage from another person, compelling another person to perform or to abstain from performing any act.

This definition also appears to be broad enough to address unlawful activity commonly used to facilitate financial crimes such as change of banking details fraud, which entails a cybercriminal intercepting emails between innocent parties and altering information, such as banking details, thereby facilitating the erroneous and fraudulent transfer of funds into an alternate bank account.

Cybercrime reporting obligations

Of note is that both electronic communications service providers (ECSPs) and financial institutions (FIs) are required to fulfil reporting obligations and assist law enforcement authorities to investigate cybercrimes.

Both ECSPs and FIs in control of data, computer programs, computer data storage mediums or computer systems that are subject to a search by law enforcement authorities must, if required, provide technical or other reasonably necessary assistance to a police official or investigator in order to search for, access or seize an article. Failure to do so is an offence, and exposes ECSPs and FIs, upon conviction, to a fine or imprisonment for a period not exceeding two years, or to both a fine and such imprisonment.

THE CYBERCRIMES ACT: Cyber fraud and private sector reporting obligations

Section 54 of the Cybercrimes Act obliges ECSPs and FIs that are aware or become aware that their service or electronic communications network is involved in the commission of a cybercrime (in respect of a category or class of prescribed reportable cybercrimes) to, without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report it in the prescribed form and manner to the South African Police Service (SAPS) and preserve any information which may be of assistance to the SAPS in investigating the offence. The form and manner of reporting is yet to be published in the Government Gazette. Failure to comply with the reporting obligation is an offence and ECSPs or FIs will, upon conviction, be liable to a fine not exceeding R50,000.

This reporting obligation does not, however, impose any obligation on ECSPs or FIs to actively monitor the data that they process for any unlawful activity. Therefore, all ECSPs and FIs are advised to ensure that they build appropriate procedures into their cybersecurity and incident management protocols to ensure that they are able to achieve compliance with this reporting obligation on an ongoing basis.

The significant increase in both the number and seriousness of cybercrime-related incidents in South Africa in recent times, including attacks on banks and municipalities and on the ports authority, amplifies the importance of the Cybercrimes Act in South Africa.