SMD Group
IP Services and Products

SMD **Country Index** ARTICLE

Recent Legal Development in Kenya - Enactment of the Computer Misuse and Cybercrimes Act, 2018

By Andrew Ndikimi, O&M Law LLP, Kenya

BRIEF SUMMARY ON THE COMPUTER MISUSE AND CYBERCRIMES ACT, 2018

INTRODUCTION:

The President of the Republic of Kenya assented to The Computer Misuse and Cybercrimes Act, 2018 (the "**Act**") on 16th May 2018. Below is a summary of its provisions:

Objectives of the Act

The Act was to provide for a framework to prevent and control the threat of cybercrime, i.e. offences against computer systems.

The Act stipulates its objectives as:

(1) Protecting the confidentiality , integrity and availability of computer systems, programs and data;

(2) Prevent the unlawful use of computer systems (including mobile devices);

(3) Facilitate the investigation and prosecution of cybercrimes; and

(4) Facilitate international/states cooperation on matters provided for under the Act.

Establishment of the National Computer and Cybercrimes Co-ordiantion Committee

The Act provides for the establishment of the National Computer and Cybercrimes Co-ordiantion Committee, whose functions shall be *inter alia*:

a) Advising the Government on security related aspects relating to blockchain technology, critical infrastructure, mobile money and trust accounts;
b) Advise the National Security Council of computer and cybercrimes;
c) Co-ordinate national security organs on matters related to computer and cybercrimes;
d) Receive and act on reports relating to computers and cybercrimes;
e) Develop a frame work to facilitate the availability, integrity and confidentiality of critical national information infrastructure;

f) Co-ordiante collection and analysis or cyber threats and respond to cyber incidents that threaten Kenya's cyberspace; and
g) Establish codes of cyber-security practice and standards of performance for implementation by owners of critical national information infrastructure.

OFFENCES AND PENALTIES/ PUNISHMENT:

The Act introduces numerous offences related to computers, computer systems, data, storage media, telecommunication devices, hand held devices etc and prescribes the punishment for each such offence. Some of the offences introduced by the Act include the following:

1) Unauthorised access to computer systems;
2) Access to computer systems with intent to commit a further offence;
3) Unauthorised interference to a computer system, program or data;
4) Unauthorised interception of data, computer programs, computer systems etc;
5) Manufacture, selling, importation, supply, distribution etc of illegal devices, programs, passwords, access codes etc;
6) Unauthorised disclosure of passwords or access codes;
7) Cyber Spying and cyber espionage;
8) False, misleading or fictitious publication of data or information with intent that such data be acted upon as authentic;
9) Publishing of child pornographic material through a computer system;
10) Computer forgery;
11) Computer fraud;
12) and fraud;
13) Cyber harassment (cyber stalking and cyber-bullying);
14) Cybersquatting;
15) Identity theft and impersonation;
16) Phishing;
17) Interception of electronic messages or money transfer;
18) Willful misdirection of electronic messages;
19) Cyber terrorism;
20) Inducement to deliver electronic message;
21) Intentionally withholding message delivered erroneously;
22) Unlawful destruction of electronic messages;
23) Wrongful distribution of obscene or intimate messages;
24) Fraudulent use of electronic data;
25) Issuance of false e-instructions;
26) Failure to report cyber threat; and
27) Failure by an employee to relinquish access codes.

The Act also makes it an offence for any person to aid or abet any person in the commission of any crime and criminalized attempting to commit any crime (attempt to commit an offence) and provides for the punishment in both instances.

The Act provides for stiff penalties in relation to computer systems related offences.

We have discussed the ingredients of each of these offences and their punishments below:

1) Unauthorised access:

The Act stipulates that a person who causes a computer system to perform a function infringing security measures, with intent to gain unauthorised access (and knowing that the access is unauthorised) commits an offence. The punishment for this is a fine **not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**. The Act define "**unauthorised access**", as access by a person to a computer system where the person: (i) is not entitled to control or access such computer system, program or data; and/or (ii) does not have consent from any person who is entitled to access the computer system through any function to the program or data.

2) Access with intent to commit a further offence

A person who commits any offence, with intent to commit a further (second) offence/crime, or facilitates the commission of such a further (second) offence also commits an offence. The punishment for this is a fine **not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 10 years, or both**.

3) Unauthorised interference

Any person who intentionally and without authorisation does any act which causes an unauthorised interference to a computer system, program or data commits and offence. The punishment for this is a fine **not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 5 years or both**. The Act defines 'unauthorised interception/ interference' as where such offender: (i) is not legally entitled to cause such interference; or (ii) does not have consent to interfere with such computer system, data etc, from a person with legal authority to do so. Further any person who commits such offenses, and the offence leads to significant financial loss to any third party, threat to national security, causes physical injury or death to any third party or causes threat to public health or public safety is liable to **a fine not exceeding Kshs. 20,000,000/- or imprisonment for a term not exceeding 10 years, or both.**

4) Unauthorised interception

The Act also criminalizes intentional and unauthorised interception of transmission of data to or from a computer system over a telecommunication system. The punishment for this is **a fine not exceeding**

Kshs. 10,000,000/- or imprisonment for a term not exceeding 5 years, or both. In addition, where such an offence leads to significant financial loss to any third party, threat to national security, causes physical injury or death to any third party or causes any threat to public health or public safety, such a person shall be liable **to a fine not exceeding Kshs. 20,000,000/- or imprisonment for a term not exceeding 10 years, or both**.

5) Illegal devices, programs, passwords and access codes etc

The Act criminalizes the manufacture, adaption, selling, procurement, importation, supplying, distribution and/or availing of any device, program, computer password, access code or similar data (collectively referred to as "**Illegal Devices and Access Codes**") designed or adapted primarily for purpose of committing any offence under the Act. The punishment for this is **a fine not exceeding Kshs. 20,000,000/- or imprisonment for a term not exceeding 10 years, or both**. Further any person who knowingly receives or is found in possession of any Illegal Devices and Access Codes with intent to use the same for hacking (without sufficient justification or excuse) shall be liable to **a fine not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 5 years, or both**. However, no offence is committed where a person found with such Illegal Devices and Access Codes can demonstrate that the same was: (i) for any legal and authorised training, testing or protection of a computer system; or (ii) undertaken pursuant to a court order or pursuant to the Act. Such therefore would be defences in such a case.

6) Unauthorised disclosure of password or access code

The Act also criminalizes unauthorised disclosure of any passwords, access codes or other means of gaining access to any program or data held in any computer system. The punishment for this is **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**. Further, any person who commits such an offence for any wrongful/unlawful gain to himself, unlawful purpose or to occasion any loss to any third party shall be liable to **a fine not exceeding Kshs. 10,000,000/- or imprisonment for term not exceeding 5 years, or both**.

7) Cyber spying and cyber espionage

The Act now criminalizes cyber spying and cyber espionage. This is what is commonly known as 'hacking'. The Act provides a very stiff penalty for this. It provides stiff and prohibitive imprisonment term and fine for criminalizes cyber spying or cyber espionage. It stipulates that any person who gains unauthorized access to critical data, datatbase or information infrastructure or without authority intercepts such data is guilty of an offence whose punishment **is a fine not exceeding Kshs. 10,000,000/- or imprisonment for a term not exceeding 20 years, or both**. Further, it provides that if any person commits this offence and it causes physical injury to any person, the punishment for the

same will be imprisonment for **a term not exceeding 20 years**. Further, it provides that any person who unlawfully and intentionally undertakes cyber spying or cyber espionage to directly or indirectly benefit a foreign state/country against the Republic of Kenya, the same is punishable by imprisonment for **a term not exceeding 20 years or a fine not exceeding Kshs. 10,000,000/-, or both**.

In addition, any person who allows another person to undertake cyber spying or cyber espionage for the direct or indirect benefit of a foreign state against the Republic of Kenya, shall be liable to imprisonment for **a term not exceeding 10 years or a fine not exceeding Kshs. 5,000,000/- or both**.

8) False publication (publishing false news)

The Act also criminalizes publishing false, misinforming, misleading or fictitious data or misinforming with intent that the data shall be considered or acted upon as authentic/true. The punishment for this is imprisonment for **a term not exceeding 2 years or a fine not exceeding Kshs. 5,000,000/-, or both**. The Act provides that the freedom of expression under the Constitution shall be limited in respect of intentional publication of such false information which is likely to propagate war, incite persons to violence, advocates hatred that *inter alia* constitutes ethnic incitement, vilification of others or is based on any ground of discrimination as stipulate in the Constitution.

On 18th May 2018, the Machakos County Governor Dr. Alfred Mutua published a tweet stating that he had already lodged a complaint at Ogembo Police Station, under the Act, against a Standard Media Group journalist, Mr. Geoffrey Mosuku, claiming that the journalist published false news about him[1]. It will be interesting to see how the Kenya Police will handle this complaint as it might be the first investigation and/or prosecution by the Kenya Police and/or the office of the director of public prosecution, under the Act.

9) Publication of false information in print, broadcast etc

The Act provides that any person who knowingly publishes information that is false in print, broadcast, data or over a computer system that is calculated to result in panic, chaos or violence amongst Kenyans or is likely to discredit the reputation of any person is liable to **a fine not exceeding Kshs. 5,000,000/- or a fine not exceeding 10 years or both**.

10) Child pornography

The Act further criminalizes child pornography. It provides that any person who intentionally publishes child pornography through a computer system, produces child pornography for purpose of its publication through a computer system or is found in possession of child pornographic material in a

[1] Please see https://twitter.com/DrAlfredMutua/status/997444999125110785 , https://twitter.com/DrAlfredMutua/status/997446032068874241 and https://twitter.com/DrAlfredMutua/status/997451588884148224

computer system or data storage medium, shall be liable to imprisonment for **a term not exceeding 25 year or a fine not exceeding Kshs. 20,000,000/-, or both**[2]. However, the Act provides that it shall be a defence if such a person establishes that a publication was justified as being for the public good on the grounds that such book, pamphlet, paper, writing, drawing, painting, art, representation or figure was in the interest of science, literature, learning or other objects of good concerns. The Act defines a "**child**" as any person below the majority age. "**Child pornography**" includes both visual and audio data.

11) Computer forgery.

Any person who commits computer forgery, through **intentional** input, alteration, deletion or suppression of computer data resulting in inauthentic/false/incorrect data, with an intent that it be considered as authentic/true, is guilty of a criminal offence. The punishment for this is **imprisonment for a term not exceeding 5 years or a fine not exceeding Kshs. 10,000,000/-, or both**. Further, any person who undertakes computer forgery for wrongful/unlawful gain, wrongful loss to another person or for economic benefit to himself or another person, is liable to imprisonment for **a term not exceeding 10 years or a fine not exceeding Kshs. 20,000,000/-, or both**.

12) Computer fraud

The Act also prohibits computer fraud. It states that any person who fraudulently and dishonestly unlawfully gains, occasions unlawful loss to another person or obtains economic benefit for himself or for another person through computer fraud is guilty of an offence. The punishment for this is **imprisonment for a term not exceeding 10 years or a fine not exceeding Kshs. 20,000,000/-, or both**.

13) Cyber harassment (cyberstalking and cyber-bullying)

The Act prohibits cyber stalking and cyber bullying. Cyberstalking and cyber-bullying has been a big problem in Kenya especially on social media and has even lead victims to committing suicide in certain instances[3]. It provides that any person who, individually or with others, willfully and repeatedly communicates, directly or indirectly, with another person knowing that such communication: (i) is likely to cause such a person apprehension or fear of violence to them or damage or loss on that person's property; or (ii) will detrimentally affect that person, commits an offence whose punishment is **imprisonment for a term not exceeding 10 years or a fine not exceeding Kshs. 20,000,000/-, or both**. The Act therefore puts cyber stalkers and cyber-bullies on notice as the punishment for such is a severe fine and a prolonged imprisonment term. Further, the Act provides that a person may apply to court for an order compelling a person charged with such an offence to refrain from engaging or attempting to engage in or enlisting the help of another person to engage in any communication complained of. Further, the Act provides that the court may order a service provider to provide any

[2] Please see https://www.nation.co.ke/news/Posting-Photos-Naked-Children-Online-/1056-4572202-p1ma5n/index.html
[3] Please see https://nairobinews.nation.co.ke/life/cyber-bullying-womans-suicide/

subscriber information in it possession for the purpose of identifying a person whose conduct is complained of. In addition, it stipulates that anyone who violates or contravenes a such a court order commits an offence and is liable to **a fine not exceeding Kshs. 1,000,000/- or imprisonment for a term not exceeding 6 months, or both**.

14) Cybersquatting

The Act provides that any person who intentionally takes or makes use of a name, business name, trade mark, domain name or other registered word or phrase owned or used by another person on the internet or in any other computer network, without the owner's authority is liable to **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

15) Identity theft and impersonation

The Act provides that any person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature belonging to another person is liable to **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

16) Phishing

The Act provides that any person who creates or operates a website or sends a message through a computer system with intention to induce a user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system is liable to **a fine not exceeding Kshs. 300,000/- or imprisonment for a term not exceeding 3 years, or both**.

17) Interception of electronic messages or money transfer (e.g. mobile money transfer)

The Act provides that any person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed is liable to a fine not exceeding 200,000/- or imprisonment for a term not exceeding 7 years, or both.

18) Willful misdirection of electronic messages

It provides that any person who willfully misdirects electronic messages I liable to **a fine not exceeding Kshs. 100,000/- or imprisonment for a term not exceeding 2 years, or both**.

19) Cyber terrorism

The Act stipulates that any person who accesses or causes to be accessed a computer or computer system or network for purposes of carrying out a terrorist act is liable to **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 10 years, or both**.

20) Inducement to deliver electronic message

The Act provides that any person who induces a person in charge of electronic devices to deliver an electronic message not specifically meant for him is liable to a fine not exceeding **Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

21) Intentionally withholding message delivered erroneously

The Act provides that any person who intentionally hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by that person or delivered to that person in error is liable for **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

22) Unlawful destruction of electronic messages

The Act provides that any person who unlawfully destroys or aborts any electronic mail or process through which money or information is being conveyed is liable to **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

23) Wrongful distribution of obscene or intimate images

Any person who transfers, publishes or disseminates through a telecommunication network or through any other means an intimate or obscene image of another person is liable to **a fine not exceeding Kshs. 200,000/= or imprisonment for a term not exceeding 2 years, or both**.

24) Fraudulent use of electronic data

The Act provides that any person who:

(i) knowingly and without authority causes loss of any property by altering, erasing, inputting or suppressing any data;
(ii) sends an electronic message which materially misrepresents any facts, leading to damage or loss by the person relying on the contents of such message;

(iii) with intent to defraud, franks electronic messages, instructions, subscribes any electronic message or instructions; or

(iv) manipulates a computer or other electronic payment device with intent to short pay or overpay;

is liable to **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both.**

25) Issuance of false e-instructions

The Act stipulates that any person authorized to use a computer or other electrical device for financial transactions issues fake electronic instructions is liable to **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

26) Failure to report a cyber threat

Any person who operates a computer system or network, whether public or private, should immediately report any attacks, intrusions and other disruptions to the functioning of any computer system or network within 24 hours of such attack, intrusion or disruption. Failure to report such attack, intrusion or disruption is an offence punishable by **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

27) Failure by an employee to relinquish access codes

The Act stipulates that an employee who fails to relinquish all codes and access rights to their employer's computer network or system immediately upon termination of his employment is liable to **a fine not exceeding Kshs. 200,000/- or imprisonment for a term not exceeding 2 years, or both**.

In addition to the above twenty seven (27) offences introduced by the Act, the Act also provides as follows:

Aiding or abetting in the commission of an offence under the Act

The Act criminalizes assisting, aiding or abetting a third party in the commission of a computer systems related offence. It stipulates that any person who knowingly and willfully assists another person to commit any offence is liable **to imprisonment for a term not exceeding 4 years or a fine not exceeding Kshs. 7,000,000/-, or both**.

Attempt to commit an offence

The statute also criminalizes any attempt to commit a computer systems related offence. Any attempt (willingly and knowingly) by any person to commit an offence under the Act is punishable by **imprisonment for a term not exceeding 4 years or a fine not exceeding Kshs. 7,000,000/-, or both**.

Offences by body corporates

The Act treats corporate offenders differently from individual offenders and provides a stiffer penalty (fine) for corporate offenders. It provides that if an offence under the Act is committed by a body corporate (e.g. a company, association and government body, institution), such body corporate shall be liable to **a fine not exceeding Kshs. 50,000,000/-**. The Act also makes principal officers of such corporate offenders culpable of any offence committed by the corporate where they were aware of the same or failed to exercise due diligence to prevent the same. It provides that the principal officers of such body corporates (unless they prove that the offence was committed without their knowledge or consent and that they exercised due diligence to prevent the commission of the offence) will be liable to imprisonment for **a term not exceeding 3 years or a fine not exceeding Kshs. 5,000,000/-, or both**.

Confiscation or forfeiture of assets and compensation of victims

The Act provides that a court may order the confiscation or forfeiture of monies, proceeds, properties and assets purchased or obtained with proceeds derived from the commission of an offence under the Act. Further, the court may make an order for compensation to any person who suffers loss from the commission of any of the above discussed offences.

OTHER RELEVANT PROVISIONS:

Search with warrants

The Act gives certain powers to police officers (or any other person authorised by law), having reasonable grounds to believe that there may be a certain computer system, data or program that is required for any investigations or legal proceedings or acquired pursuant to commission of an offence. Such officers are allowed to apply to court for search warrant to enter any premises for purposes of accessing, searching and seizing such data. However, such an officer must satisfy the court: (i) as to the reason why he believes that such material may be found at the premises to be searched; (ii) show that the search may be frustrated or seriously prejudiced unless an investigating officer may at the first instance on arrival at the premises secure entry to the premises; (iii) identify and explain the type of evidence sought; and (iv) explain measures that shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as imaging, mirroring or copying of relevant data and not through physical custody of computer system, program , data or storage medium.

Search without a warrant

Further, the Act allows such investigating officers to search such premises without a warrant where the officer suspects that an offence has been committed and to take possession of such computer system.

The Act further allows a police officer, where he has reasonable grounds to believe that there is any data stored in any computer system which is required for a criminal investigation or there is risk or is vulnerable to be modified, deleted, lost or destroyed or rendered inaccessible, to serve notice on any person in possession of such data requiring such a person to preserve such data or disclose it to him.

Telecommunications Service providers

The Act also allows any police officer, pursuant to a court order, to have access to traffic data of any telecommunications service provider (e.g. mobile network providers) and collect or record such data, where he has reasonable ground to believe that such data is required for investigations.

The court in giving such orders must ensure that the police officer: (i) states the grounds upon which he believes that the data sought is available; (ii) states the type of data sought; (iii) identifies and explain the subscribers, users or unique identifiers of the subject; (iv) states the identifiable offences suspected to have been committed; and (v) explains the measures he will take to prepare and ensure that the data will be procured while maintaining the privacy of other users, customers and third parties and without disclosure of data to any party who is not a part of such investigating team. Failure by a service provider to comply with such orders, **in the case of a corporation will be liable to a fine not exceeding Kshs. 10,000,000/- and in the case of an officer of the service provider will be liable to a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**.

Obstruction of an officer

Any person who obstructs an officer undertaking his duties under the Act, including by destruction of data or failing to comply with the officer's request is liable to **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**.

Misuse of powers by a police officer

On the same breath, an officer who misuses his powers under the Act commits and offence and is liable to **a fine not exceeding Kshs. 5,000,000/- or imprisonment for a term not exceeding 3 years, or both**.

Appeals

Any person aggrieved by a decision or order of the court may appeal to the High Court or Court of Appeal (as the case may be) **within 30 days from the date of the decision or order**.

International cooperation

The Act also allows the office of the Attorney General (the Central Authority) to make a request for mutual legal assistance to a requested state (country) to investigate, collect evidence, prosecute, and repatriate any person who commits an offence under the Act. The state may also receive such a request from a requesting state.

Forfeiture

In addition to the penalties prescribed above, a court may order the forfeiture of any apparatus, device or thing that it deems appropriate to do, to the Communication Authority of Kenya, e.g. hacking devices, infringing data etc.

Suspension of numerous section of the Act by the Constitutional Court

However, on 29th May 2018, the High Court of Kenya at Nairobi, sitting as a Constitutional Court[4] , temporarily suspended the following provisions of the Act:

1) Section 5 – which deals with the Composition of the National Computer and Cybercrimes Co-ordination Committee;

2) Section 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40 and 41- which provide for the offences of: (i) unauthorized interference; (ii) unauthorized interception; (iii) false publication; (iv) publication of false information; (v) child pornography; (vi) cyber harassment; (vii) cybersquatting; (viii) identity theft and impersonation; (ix) interception of electronic messages or money transfer; (x) willful misdirection of electronic messages; (xi) cyber terrorism; (xii) inducement to deliver electronic message; (xiii) intentionally withholding message delivered erroneously; (xiv) unlawful destruction of electronic messages; (xv) wrongful distribution of obscene or intimate images; (xvi) fraudulent use of electronic data; (xvii) issuance of false e-institutions; (xviii) failing to report a cyber threat; and (xix) employees' failure to relinquish access codes, respectively;

3) Section 48 and 49 – which provides for search and seizure of stored computer data and record of an access to seized data respectively; and

4) Section 50, 51, 52 and 53- which provide for application of production order, expedited preservation and partial disclosure of traffic data, real-time collection of traffic data and interception of content data, respectively.

[4] High Court of Kenya at Nairobi, Constitutional and Human Rights Division, Petition Number 206 of 2018.

The suspension is effective until 18th July 2018 when the suit will come up for directions on the hearing of the Petition.

Conclusion

The Act introduces twenty seven (27) main offences and provides severe punishment for these offences, including huge fines and prolonged jail terms. With this new legislation, it will be interesting to see the punishment that courts will grant offenders as the punishment stipulated on the Act are the maximum punishments and courts are allowed to exercise their discretion in sentencing and most states provide for the maximum punishment.

Further, the Act is seen to be trying to cunningly reintroduce criminal defamation, which was declared unconstitutional by Hon. J. Mativo in the decided case of **Jacqueline Okuta & another –vs- Attorney General & 2 others**[5] as it offended the Constitutional right to freedom of speech.

It will be interesting to see how the Act will be implemented given that already there are constitutional petitions challenging the Act as it limits fundamental rights and freedom enshrined in the Constitution and further some sections of the Act have temporarily been suspended by the Constitutional Court.

For more information, please contact:

The author is a Kenyan advocate with ten (10) years post admission experience and is a senior lawyer specializing in intellectual property law, commercial law, ICT law, entertainment law and media law at O&M Law LLP, Park Place, Limuru Road & 2nd Parklands Avenue Junction, Nairobi, Kenya.

Telephone: +254722613888/ +254739935929
Email: andrew@omlaw.co.ke
Website: www.omlaw.co.ke

[5] High Court at Nairobi Constitutional Petition Number 397 of 2016 [2017]eKLR

ADVOCATES | COMMISSIONERS FOR OATHS | NOTARIES PUBLIC

4th Floor, Park Place Limuru Road /2nd Parklands Avenue
P. O. Box 49393 - 00100, Nairobi, Kenya
Dropping Zone No. 35, Revlon Professional Plaza, Tubman Road
Tel: (+254 20) 2323836/9, 0720 994 511
Fax: (+254 20) 2323846
Email: info@omlaw.co.ke
Mobile: 0720 994 511 / 0736 520 767