the Above Standard

A PUBLICATION OF TRIPLEOKLAW ADVOCATES

ISSUE 001
JUNE 2018

WIN AGAINST

THE COMPUTER MISUSE

& CYBERCRIMES ACT, 2018

TRIPLEOKLAW ADVOCATES

the Above Standard

MAY • ISSUE 001 • 2018

SPECIAL 1ST EDITION

PUBLISHER
TripleOKLaw Advocates LLP.

EDITOR
Catherine Kariuki Mulika

EDITORIAL TEAM
Evance Odhiambo
Franklin Cheluget
Janet Othero
Kenvine Ouma
Kivindyo Munyao
Leyla Ahmed
Mbula Nzuki
Renice Midar
Stephen Mallowah
Tom Onyango

ART & DESIGN
Smith Creative.

FOR FREE SUBSCRIPTION, go to
www.tripleoklaw.com

TRIPLEOKLAW ADVOCATES

ACK Garden House, 5th Floor, Wing C
First Ngong Avenue, off Bishops Road,
P. O. Box 43170 - 00100, Nairobi, KE
Pilot Telephone: +254 20 272 7171
Email: info@tripleoklaw.com
Web: www.tripleoklaw.com

IN THIS ISSUE

IN THIS ISSUE

COVER STORY

REGULARS

Editor's Note

Welcome to the inaugural issue of *The Above Standard,* our new quarterly newsletter. Our aim is to have a newsletter that is entertaining, informative and above all useful to the readers. Being our maiden issue, we dedicate it to our esteemed clients, friends of TripleOKLaw Advocates LLP and our dedicated staff who have tirelessly worked to transform the ideas into a beautiful reality. In this issue, our Advocates and Trainee Advocates have collaborated to write on an array of topical practice issues ranging from: the new Computer Misuse and Cybercrimes Act, 2018; constructive dismissal in the workplace; double jeopardy in cross-border crimes; risk allocation in PPPs; digitization of land records; and investment bank's fiduciary duties. We also provide quirky and light-hearted insights into some of our advocates here at TripleOKLaw.

We hope that all our readers will turn *The Above Standard* into a source of great legal knowledge, practice insight and intellectual discourse. Enjoy this first issue, subscribe by logging into **www.tripleoklaw.com** and give us your feedback including any topics you would like to see covered in the future via **editorialteam@tripleoklaw.com.**

Catherine Kariuki Mulika

Managing Partner's Note

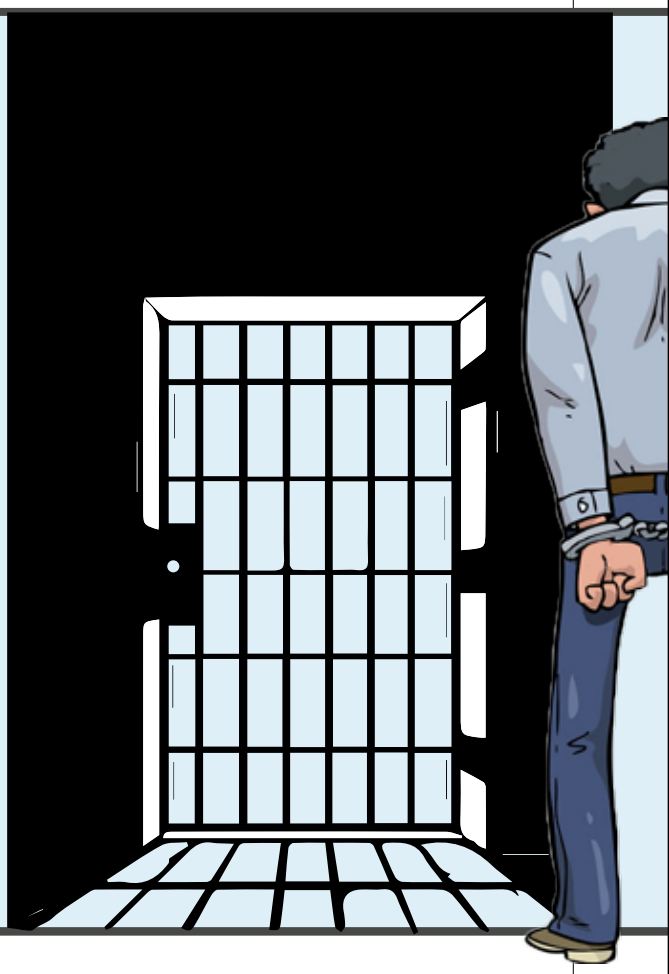
John M. Ohaga

At TripleOKlaw, we always pursue valued strategic business partnerships with our clients. We aim to provide legal solutions that offer business support. *The Above Standard* is not only a result of hard work and dedication but also a true manifestation of our credo – *going over and above* to meet our client's needs and expectations.

Once Charged, Twice Tried;

CROSS-BORDER CRIMES

James Ochieng' Oduol
Noreen Kidunduhu
Faith Netia



One of the general principles of criminal law is that one cannot be prosecuted twice for the same acts or offense. It is often referred to as the protection against "double jeopardy". The underlying objective is fair trial and finality in criminal proceedings.

This principle however poses a challenge where an act constituting a crime occurs across different jurisdictions making each jurisdiction potentially competent to investigate and prosecute the same crime. Which state has primary duty to prosecute? Are the other states barred from proceeding with charges where there has been a conviction or an acquittal in one of the states in which the crime was committed?

Strict Application

With increase in international corporate crime, cybercrime and transnational crime such as corruption, a strict application of the principle would mean that

> **This strict application of the principle pits the right to be free from multiple prosecutions against the right of a sovereign state to enforce its laws.**

there can only be a single enforcement action in a sole forum but where only the interests of the prosecuting state are represented.

This strict application of the principle pits the right to be free from multiple prosecutions against the right of a sovereign state to enforce its laws. It undermines the affected states' sovereignty by requiring them to surrender their power to prosecute criminal conduct in a bid not to offend the double jeopardy principle. It is indeed quite absurd for a national court to be prevented from dealing with criminal misconduct within its jurisdiction despite there being a genuine public interest in it doing so. It has also been argued that a strict application of the rule could encourage forum shopping by culpable persons which may result in undesirable outcomes.

International Practice

Whilst most countries have enshrined the principle of double jeopardy in their criminal laws, there is no universal acceptance of an equivalent international rule, i.e. prohibiting prosecution of the same criminal conduct in multiple jurisdictions. The UK and many European states recognize the rule and will decline to prosecute conduct which has previously been prosecuted in another jurisdiction.

The US on the other hand does not. In the case of United States of **America (USA) Vs Gi- Hwan Jeong,**[1] Gi- Hwan Jeong a South Korean national was charged with bribing American public officials in exchange for their aid in securing a lucrative telecommunications contract. To ensure that he submitted the winning bid for the AAFES (The Army & Air Force Exchange Service) contract, Jeong agreed to pay $20,000 in exchange for confidential information that enabled him to secure the contract in November 2001. He later paid more money in the subsequent years to maintain the relationship with AAFES. The accused however, sought a dismissal of the prosecutions on grounds that he had been previously convicted and fined in South Korea. The Court in upholding the conviction observed that the federal bribery laws have extraterritorial application, and that the Convention was neither self-executing nor a bar to multiple prosecutions. On appeal, the appellate Court upheld the decision of the trial court and noted that no applicable international law had been pointed to the court that limited the United States' jurisdiction over the offenses in the case.

Kenyan Context

The basis of the principle of double jeopardy is found in Article 14(7) of the International Covenant on Civil and Political Rights (ICCPR) and which is adopted in Kenya by virtue of Article 2(5) of the Constitution.

Article 50 (2) of the Constitution also provides for the principle as follows:

Every accused person has the right to a fair trial, which includes the right:

(o) not to be tried for an offence in respect of an act or omission for which the accused person has previously been either acquitted or convicted

The principle also finds place in Section 279 of the Criminal Procedure Code.

As far as international double jeopardy is concerned, under Article 124(5) of the East African Community Treaty, the partner states agree to enhance co-operation in the handling of cross border crime and provision of mutual assistance in criminal matters. There are also several laws governing extradition in Kenya. The Extradition (Commonwealth Countries) Act makes provisions for Kenya to surrender to other Commonwealth countries on a reciprocal basis, persons accused or convicted of offences in those countries. The Extradition (Contiguous and Foreign Countries) Act consolidates the law concerning the extradition of offenders and related matters, where Kenya has an agreement with a non-Commonwealth country. The Fugitive Offenders Pursuit Act authorizes the police of Uganda and Tanzania to pursue within Kenya offenders who are fugitive from those countries where there are reciprocal arrangements with Kenya.

Other than these, Kenya has not taken a stand on whether or not it recognizes an international variant of the double jeopardy principle, but this will soon become necessary with the recent spike of cross border crime. It is notable that Kenya has recently enacted the Computer Misuse and Cybercrimes Act which addresses cross border crimes.

Measured Co-ordination

With the upsurge of cross border crime, it will become increasingly common that one incident of alleged misconduct will trigger years of parallel or successive enforcement actions and, in some cases, duplicative penalties by different authorities. When overlapping jurisdiction exists, and states proceed in isolation, what can result is an unfair, unpredictable, and overly punitive regime that, in the long run, may prove counterproductive.

There is need for a solid enforcement comity, with solemn rules of communication and co-operation between states which will determine which state proceeds with the prosecution, the criminal penalties to be imposed and how they will be apportioned. This will eliminate the possibility of multiple prosecutions and ensure all affected parties are accorded justice by involving all interested states in the investigatory and prosecutorial stages of the case.

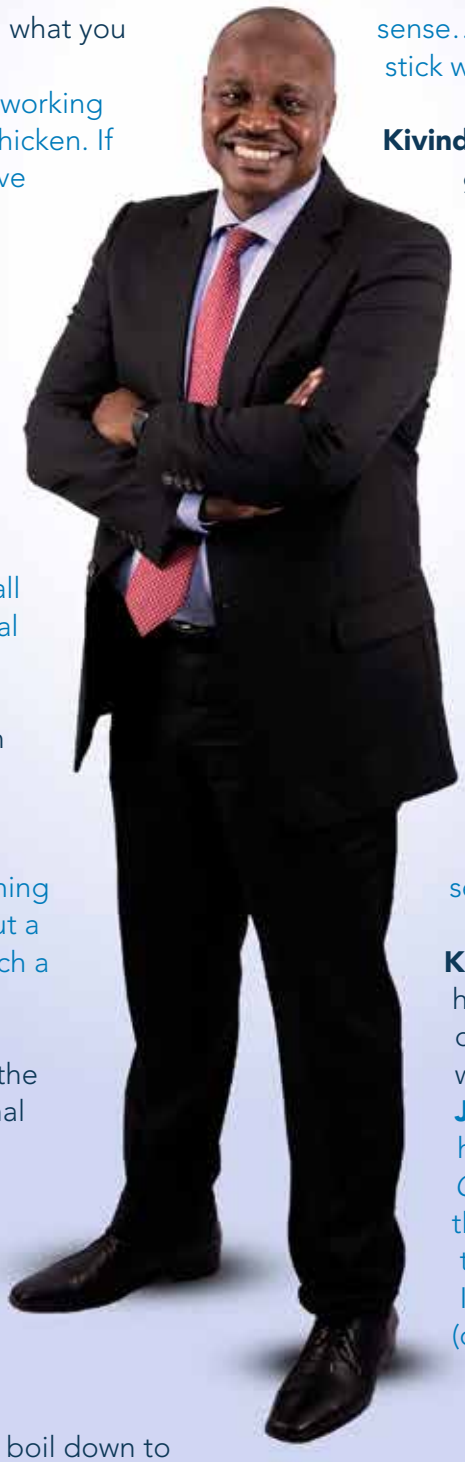
When overlapping jurisdiction exists, and states proceed in isolation, what can result is an unfair, unpredictable, and overly punitive regime that, in the long run, may prove counterproductive.

For more information on this, contact James Ochieng' Oduol
jochieng@tripleoklaw.com

KNOW YOUR ADVOCATE

James Ochieng' Oduol aka J.O.O

Interviewer: Kivindyo Munyao



Kivindyo: If you weren't a lawyer, what you be your alternative career?
J.O.O: I would be a farmer. I like working the soil, I like keeping *kienyenji* chicken. If farming failed, I think I would delve into different forms of business.

Kivindyo: Favorite sport?
J.O.O: I played hockey back in campus and I really enjoyed playing rugby for the Mean Machine. I played prop position. *(eyes widen with excitement)* Those were the days when Mean Machine was Mean Machine my friend! Football is my sport. I am a staunch Arsenal fan.

Kivindyo: Ever attended a match at Emirates?
J.O.O: Yes, I have. When I resided in the U.K. It was such an electrifying experience. It's one thing to watch a match on television but a completely different thing to watch a live game.

Kivindyo: Who do you consider the greatest player to wear the Arsenal Shirt?
J.O.O: Thierry Henry.

Kivindyo: Switching gears sir, in one word, how would you describe yourself?
J.O.O: Ambitious.

Kivindyo: Ambitious…Does that boil down to everything you do from the career to family?
J.O.O: Actually, yes. Or maybe stoical in a sense…but ambitious will do. I will stick with ambitious.

Kivindyo: Your daughter just graduated from University and you host a celebratory party in her honour. What drink do you serve her?
J.O.O: Rosso Nobile, of course.

Kivindyo: What informs this choice?
J.O.O: It does the trick but still leaves you sane.

Kivindyo: *(laughs)* You are well traveled, which is your favorite destination so far?
J.O.O: Dubai. It's convenient in terms of access, has a friendly environment, and offers the best things you can see in the world.

Kivindyo: If given a chance to have your last meal on earth with one guest, other than family, who would you pick?
J.O.O *(Grinning):* It would have to be J.M.O *(John Morris Ohaga)* because he would be the undertaker. He would be there to execute my last will, so I would have to be very careful. (chuckles).

WIN Against Cyber Criminals?

THE COMPUTER MISUSE AND CYBERCRIMES ACT, 2018

Catherine Kariuki Mulika
Janet Othero
Fiona Makaka
Robert Dachi

Regular cyber-attacks and attempts carried out on both private sector and government bodies are now a real threat, one that cannot be ignored and must be proactively dealt with. Successful attacks in the recent past have brought about devastating financial and reputational impacts on the victims. Increasing use of technology, digitization of systems and growing e-commerce trends mean that the number of Kenyan citizens and organizations vulnerable to cyber attacks is high. Despite its benefits, the use of technology comes with its fair share of risks.

As the use, adaptation and consumption of technology becomes more widespread, the country has become exposed to the dangers that come with its use ranging from identity theft to cyber terrorism. Even organizations with the best information security strategy have had challenges when dealing with cyber criminals after an attack since the existing criminal law was not complementary. Cyber criminals have previously exploited loopholes in the domestic laws to avoid prosecution.

Kenya has, in line with its development goals, massively invested in the information technology sector as a vehicle for economic prosperity.

The first draft of the Computer Misuse and Cybercrimes Act was initiated by a multi-governmental committee in 2015 as the Computer and Cybercrime Bill. This bill was subjected to parliamentary review and

amendment which resulted to the final version that received presidential assent on the 16th of May 2018.

Objectives of the Act

The Act aims to counter the evolution of crime through technology. It seeks to bridge the gap between advancement in technology and its regulation.

Generally, the Act addresses the following emerging issues in the cybersphere;

1. Unlawful use of computer systems;
2. Prevention, detection, investigation, prosecution and punishment of cybercrimes;
3. Protection of rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and
4. Facilitation of international cooperation on matters covered under the Act.

The Act is divided as follows;

a) Part II-National Computer and Cybercrimes Committee

The role of this committee will be to advise the government on security related in the technological field. The committee will also coordinate collection and analysis of cyberthreats for the country as well as be responsible for establishing the codes of cybersecurity practice and standards of performance for implementation by owners of critical national information infrastructure such as telecommunication service providers.

This measure is important as it acknowledges that technological infrastructure is essential to the nation and thus it creates safeguards and regulation which was previously absent in the sector. Previously, the approach to such emerging issues was spearheaded by the parent ministry in collaboration with various state agencies. Regulation was highly dependent on the industry or sector and in some instances a multi-agency approach was used.

We expect to see this committee very busy in the year as they provide regulations and guidelines on emerging issues in technology such as blockchain, cryptocurrency and artificial intelligence.

b) Part III-Offences

Prior to this Act, cybercrime offences were not exhaustively provided for in the Penal Code and other subsidiary legislation. The evolution of cyberspace has seen technology facilitating the perpetration of cybercrimes both domestically and internationally as well as aggravating the impact of the same.

Part II of the Act deals with offences and their corresponding penalties. The inclusion of the definition of offences will greatly enhance the capability of law enforcement agencies to carry out investigations and prosecute cyber criminals. The offences cut across both individual and corporate actions and omissions.

At the tail end of this article, we list a summary of the offences and their corresponding penalties.

Notably, as at the date of this article, there was a ruling issued by High Court Judge Hon. (Mr.) Chacha Mwita suspending 26 sections of this Act. The conservatory orders suspended the offences in Sections 22-24,27-29,31-41 *(highlighted in purple below)* due to the issues raised on infringement of fundamental rights

guaranteed under the Constitution.

c) Part IV-Investigative Procedures

Prior to the Act, there was no legal framework providing for the investigation and prosecution of cybercrime, specifically the collection of evidence. The Act brings certainty to a previously unexplored area of the law since it now provides for clear mechanisms in the collection of electronic evidence and investigation thereof.

Procedure relating to; search and seizure of computer data; recording of access to seized data; preservation and partial disclosure of traffic data; real time collection of traffic data and; interception of data is clearly outlined. The Honorable Court in the above-mentioned case also suspended sections 48-53 which detailed the investigation procedures to be followed.

d) Part V-International Cooperation

The global nature of technology makes it impossible for a single jurisdiction to regulate and enforce its cybersecurity laws efficiently. There is therefore a need for different countries to foster ties and facilitate collaboration in regulation and enforcement of cybersecurity law
s.
The Act at Part V seeks to address this need by providing for international cooperation between Kenyan law enforcement agencies and their colleagues from other countries to allow for the investigation of crimes that take place across multiple jurisdictions.

The Act requires that it is read together with the Extradition (Contiguous & Foreign Countries) Act, 2011 and the Mutual Legal Assistance Act, 2011 which house salient provisions for International Criminal Law.

Harmonization of these laws is essential as it allows for seamless prosecution of international crimes by law enforcement agencies. The hindrances presented by jurisdictional differences are done away with.

The Act also provides for the establishment of the Central Authority (Office of the Attorney General) which will be the main point of contact in international cooperation under the Act. This will obviously lead to better cooperation, faster and efficient investigation of crime as having a single point of contact reduces the bureaucracy that is associated with having numerous agencies carrying out similar functions.

e) Part VI-Extraterritorial Jurisdiction

Section 66 of the Act provides for the extraterritorial nature of the Act. This allows for the application of the Act outside Kenyan borders. This means that the Act can be applied to Kenyan citizens or residents carrying out crimes while outside Kenya as well as foreigners who carry out crimes against Kenyan citizens, residents and entities regardless of their geographical location.

f) Prevailing Clause

Technology cuts across a myriad of sectors possibly regulated by other laws. Section 68 of the Act has a prevailing clause which provides that the Act will supersede any other law in case of conflict.

Way forward

The Computer Misuse and Cybercrimes Act is a step in the right direction. However, it will need to be supplemented with regulations and guidelines in order to effectively address emerging issues such as Artificial Intelligence and Financial Technology which undoubtably pose a challenge to the dynamics of the regulation and enforcement of cybersecurity laws.

Summary of the offences

	OFFENCE	MAXIMUM PENALTY
14	Causing a computer system to perform a function by breaching security measures in order to gain unauthorized access. ***(computer as a tool/cracking)***	**Kshs. 5,000,000;** and/or Imprisonment for a term of **3 years**.
15	Gaining unauthorized entry into a computer system with the intention of committing an offence or aiding the commission of a crime under any law. ***(computer as a target/cracking)***	**Kshs. 10,000,000;** and/or Imprisonment for a term of **10 years.**
16	Intentional unauthorized interference to a computer system, data or program. ***(hacking)***	**Kshs. 10,000,000;** and/or Imprisonment for a term of **5 years.**
16(2)	Unauthorized interference which; • causes substantial loss to a person; or • threatens national security; or • causes death or physical injury to any person; or • threatened public safety or health.	**Kshs. 20,000,000;** and/or Imprisonment for a term of 5 years.
17(1)	Intentional and unsanctioned interception of transmission of data. It is irrelevant that the interception was not targeting any system, program or data. (illegal interception/ wire tapping)	**Kshs. 10,000,000;** and/or Imprisonment for a term of **5 years.**
17(2)	Intentional and unsanctioned interception of transmission of data which; • causes substantial loss to a person; or • threatens national security; or • causes death or physical injury to any person; or • threatens public safety or health.	**Kshs. 20,000,000;** and/or Imprisonment for a term of **10 years.**
18	Knowingly dealing or making available devices, programs or access codes on the basis of committing a crime. The exception to this is only when the acts were intended for the sanctioned training, testing or protection of a system and the use of the access codes or passwords were done in accordance with the law. *(virus dissemination)*	**Kshs. 20,000,000;** and/or Imprisonment for a term of **10 years.**
19	Intentional and unauthorized disclosure of access codes or passwords.	**Kshs. 5,000,000;** and/or Imprisonment for a term of **3 years.**
19 (2)	Intentional and unauthorized disclosure of access codes or passwords; • for any wrongful gain • for unlawful purpose • to occasion any loss	**Kshs. 10,000,000;** and/or Imprisonment for a term not exceeding **5 years.**

	OFFENCE	MAXIMUM PENALTY
20	Committing the above-mentioned offences on a protected computer system.	**Kshs. 5,000,000;** and/or Imprisonment for a term of **20 years.**
21(1)	Performing an act intentionally and unlawfully or allowing a person to commit a prohibited act for the purposes of accessing critical information or intercept data from a critical information center.	**Kshs. 10,000,000;** and/or Imprisonment for a term of **20 years.**
21(2)	Committing an offence mentioned above and causing physical injury to a person.	Imprisonment for a term of **20 years.**
21(3)	Committing an offence mentioned above and causing death of a person.	Imprisonment for life.
21(4)	Unlawful and intentional remittance or receipt of data from a critical information center with intent to benefit a foreign state to the detriment of Kenya. *(cyber espionage)*	**Kshs. 10,000,000;** and/or Imprisonment for a term of **20 years.**
21(5)	Intentional publication of false information that misinforms and with the intention that the false information shall be acted upon. The misleading information can be that which can insight violence, cause war, hate speech or propagate incitement. *(information warfare)*	Kshs. 5,000,000; and/or Imprisonment for a term of **2 years.**
23	Publishing of false information in print, broadcast, data or over a computer system that leads to violence or panic and which is likely to tarnish a person's reputation. (fake news)	**Kshs. 5,000,000;** and/or Imprisonment for a term of **10 years.**
24	Intentional publishing, production, circulation, sale or possession of child pornography in a computer or another storage medium. Child pornography includes data that portrays; • a child engaged in sexually explicit conduct • a person who appears to be a child engaged in sexually explicit conduct • images representing a child engaged in sexually explicit conduct	**Kshs. 20,000,000;** and/or Imprisonment for a term of **5 years.**
25	Intentional inputting, alteration, deletion or suppression of computer data with the intention that it would be acted upon as if it was authentic. Committing the offence stated above with intent of wrongful gain, loss to another person or for economic benefit.	**Kshs.10,000,000;** and/or Imprisonment for a term of **5 years.** **Kshs. 20,000,000;** and/or Imprisonment for a term of **10 years.**

	OFFENCE	MAXIMUM PENALTY
26	Unauthorized access, alteration of data, interference, transfer or use of any data with the intent of wrongful gain, loss to another person or for economic benefit. *(ransomware)*	**Kshs. 20,000,000**; and/or Imprisonment for a term of 10 years.
27	Communication by a person with another party if aware or ought to be aware that the person's conduct may cause damage or affects that party in a negative way or is offensive in nature. (Cyber harassment)	**Kshs. 20,000,000;** and/or Imprisonment for a term of **10 years.**
28	Unauthorized intentional use of another person's duly registered or owned name, business name, trademark, domain name on the internet. (copyright infringement, passing off, cybersquatting)	**Kshs. 200,000;** and/or Imprisonment for a term of **2 years.**
29	Use of an electronic signature password or identification feature dishonestly.	**Kshs. 200,000;** and/or Imprisonment for a term of **3 years.**
30	Creation or operating a website and sending a message through a computer system with the intention of prompting the user to disclose personal information. *(phishing)*	**Kshs. 300,000;** and/or Imprisonment for a term of **3 years.**
31	Destroying or aborting electronic mail or any process where money information is being transmitted.	**Kshs. 200,000;** and/or Imprisonment for a term of **7 years.**
32	Intentionally misdirecting electronic messages.	**Kshs. 100,000;** and/or Imprisonment for a term of **2 years**.
33	Accessing or causing access to a computer system for the purposes of committing a terrorist act. *(cyber terrorism)*	**Kshs. 5,000,000;** and/or Imprisonment for a term of **10 ye**ars.
34	Prompting a person in charge of an electronic device to deliver electronic messages not meant for that person.	**Kshs. 200,000;** and/or Imprisonment for a term of **2 years.**
35	Hiding or detaining any electronic mail, message, electronic payment, credit and debit card that has been delivered by mistake from the intended person.	**Kshs. 200,000;** and/or Imprisonment for a term of **2 years.**
36	Unlawful destruction or aborting of any electronic mail or processes through which transmission of money or information is done.	Kshs. 200,000; and/or Imprisonment for a term of **2 years.**

	OFFENCE	MAXIMUM PENALTY
37	Transfer, publishing, dissemination or transmission in any manner for distribution or downloading through a computer system of intimate or obscene images of another person. (obscenity, (revenge) pornography & cyber bullying)	**Kshs. 200,000;** and/or Imprisonment for a term **of 2 years.**
38	i) Knowingly causing loss of property to another by altering, erasing, inputting or suppressing data; ii)Sending electronic messages which materially misrepresents facts which upon reliance causes damage or loss; iii)Franking electronic messages, instructing super scribing electronic messages or instructions with intent to defraud; iv)Manipulation of a computer or electronic payment device with the intention on overpaying or short paying. *(data diddling)*	**Kshs. 200,000;** and/or; Imprisonment for a term of **2 ye**ars.
39	Use of a computer or electronic device by an authorized person for financial transactions issuing false electronic instructions.	**Kshs. 200,000;** and/ or Imprisonment for a term of **2 years.**
40	Failure to report cyber threats, attacks or intrusions by a person who operates a computer system or network. *(reporting breaches)*	**Kshs. 200,000;** and/or Imprisonment for a term of **2 years.**
41	Employee failure to relinquish all access rights to their employer.	**Kshs. 200,000** and/or Imprisonment for a term of **2 years.**
42	Knowingly aiding and abetting the commission of an offence under the Act.	**Kshs. 7,000,000** and/or Imprisonment for a term of 4 years.
43	A body corporate committing an offence under the Act.	**Kshs. 50,000,000** for the body corporate **Kshs 5,000,000** for any principal who committed the offence; or **Forfeiture** of assets, monies or proceeds
48	Where a police officer or authorized person obtains a search warrant for obtaining data intended for criminal actions and presents it to an alleged offender and there is obstruction or interference with the data being searched the alleged offender commits and offence.	**Kshs 5,000,000** and/or Imprisonment for a term of 3 years.

For more information on this,
contact Catherine Kariuki Mulika
ckariuki@tripleoklaw.com

Immigration Directive On Work Permits Issued To Foreign Nationals

Jinaro Kibet
Sherry Bor

On 21st May 2018, the Cabinet Secretary for Interior and Co-ordination of National Government gave a directive that all foreigners working in Kenya will be required to verify their work permits electronically in a biometric registration exercise. In the process, existing permits will be vetted. The exercise will be conducted over a period of 60 days ending 21st July 2018. It is expected that once the time has lapsed, sanctions will be imposed on those who haven't complied. The Immigration Department will issue electronic work permit cards.

The foreigners holding work permits are required to personally attend to the verification exercise and present a passport bearing an official endorsement, alien identification card and a Kenya Revenue Authority PIN Certificate.

This directive comes in the wake of a countrywide government crackdown on undocumented foreign workers.

All foreigners working in Kenya will be required to verify their work permits electronically in a biometric registration exercise.

For more information on this, contact Jinaro Kibet
jkibet@tripleoklaw.com

Private Money for Public Use;

RISK ALLOCATION IN PUBLIC PRIVATE PARTNERSHIPS IN KENYA

Stephen Mallowah
Bryan Muindi
Michelle Koske

Public private partnerships (PPPs) are long term contracts between a private entity and a public authority for the provision of public services or development of public infrastructure.

In return for its investment, the private party is rewarded in the form of profits while the public authority is able to fulfil its obligation to deliver the public service or public infrastructure. It is therefore of critical importance that the risks in the project are identified and properly allocated in such a manner that the interests of all parties are adequately protected.

The Public Private Partnership Act No 15 of 2013 defines a PPP in largely the same terms as set out above, and goes further to state that the private party receives a benefit for performing a public function by way of compensation from a public fund or charges or fees collected by the private party from users or consumers of a service provided to them or a combination of such compensation and such charges or fees; and is generally liable for risks arising from the performance of the function in accordance with the terms of the project agreement.

A key justification for PPPs in emerging economies is the fact that traditional public procurement requires large amounts of capital which is hard to come by. Many countries are unable to bridge the gap between available public finances and infrastructural development needs. PPPs therefore step in to mitigate this problem by allowing the public body to take advantage of the private party's strength to attract and invest capital, expertise, provision of efficient services and the need to distribute risk equitably.

A competent and stable government, coupled with the administrative capacity to effectively negotiate and manage the long term contractual relationship with the private sector is a

key prerequisite for PPPs to succeed, further underpinned by a robust legal and regulatory framework.

In these partnerships, the contracting authority either retains ownership of the project or will be entitled to ownership upon completion of the project, depending on the nature and type of the project agreement.

Legal Framework

In Kenya, PPPs are regulated by the Public Private Partnership Act, 2013, the Public Private Partnership Regulations 2014 and the PPP Project Facilitation Fund Regulations 2017.

The Act establishes the PPP Committee which approves the project proposals submitted to it by the contracting authority and ensures the efficient implementation of the project agreement entered into by the contracting authority, in accordance with the enabling legislation.

The Act has also established the PPP Unit which serves as the secretariat and technical arm of the Committee. The PPP Unit's role includes providing capacity building and advice to contracting authorities and other parties involved in the planning, coordinating, undertaking or monitoring of projects; as well as making recommendations to the Committee on the approval or rejection of projects.

It is, therefore, of critical importance that the risks in the project are identified and properly allocated in such a manner that the interests of all parties are adequately protected.

Risk Allocation in PPPs

Risks can never be eliminated but can be allocated in such a manner that both the contracting authority and private party optimally share the risks. PPP projects tend to generate more risks than traditional public procurement processes because of their complex nature. One of the guiding principles in risk allocation is a party that is best placed to manage a risk is the one who should bear it.

Risks can never be eliminated but can be allocated in such a manner that both the contracting authority and private party optimally share the risks.

These risks are broadly categorized into two types; exogenous risks, which are not in the direct control of the parties for example political risks, environmental risks, financial risks and legal risks; and endogenous risks - those that are related to the project construction and operation (for example completion risks and operation risks).

These risks can be mitigated through either insurance or reimbursements. Environmental risks can be adequately covered by insurance, while some financial risks such as in a situation where the contracting authority alters the specification of a project causing a project cost escalation would require government's compensation.

Operation risks usually borne by the private party can be mitigated by contractual guarantees from contractors and manufacturers. Political and legal risks can be mitigated through undertakings and binding letters of comfort from the government.

Governments can also provide sovereign guarantees which compel them to underwrite some of the risks and legally binds them to take on an obligation if a specified event occurs. This provides incentives to the private sector to participate in PPPs and greatly enhance the bankability of a project with lenders and investors.

In the Third Schedule of the Act, the issue of risk allocation is addressed. It stipulates the minimum contractual obligations required to be in a project agreement. The Act requires the agreement to have the basis of risk allocation in respect to the change of law, unforeseeable accidents, force majeure or discovery of antiquities, as the case may be, and the resultant compensation.

Although PPPs are not the cheapest way to deliver public services or public infrastructure, there is a trade-off between having the service or infrastructure available, albeit at a slightly higher cost, or not having it at all. There are advantages to PPPs some which include raising additional finance in a situation where there are budgetary restrictions, use of private sector operational efficiencies to reduce costs, increase of quality services to the public and the ability to speed up infrastructure development. These can be met in a situation where there is optimum risk allocation leading to a win-win situation for both the contracting authority and the private party.

For more information on this, contact Steve Mallowah
smallowah@tripleoklaw.com

Pushed to the Edge;

CONSTRUCTIVE DISMISSAL IN KENYA

John M. Ohaga
Franklin Cheluget
Mbula Nzuki

The Kenyan Employment and Labour Relations Court (ELRC) has continuously adopted a pro-employee stance in its rulings. This is informed by the notion that the employer-employee relationship is an exchange between labour and capital that tends to be characterized by inequality. By dint of this loudly pronounced stance adopted by courts in Kenya and beyond, it is of paramount importance for employers to put in place measures that ensure they remain on the right side of the law. This is not only a legal decision, but a financial/economic one too.

Constitutional Requirements of Employees

Arguably, the employment relationship is one tainted by inequality. To cure this, safe labour practices must be adopted from the onset in tandem with Article 41 of the Constitution of Kenya, 2010 which stipulates that every person has the right to fair labour practices which include: the right to fair remuneration, reasonable working conditions and to form/join/

participate in the activities and programmes of a trade union. These are understood as the bare minimum standards by which a law-abiding employer must be guided.

The Dictates of Employment Contracts in the Employment Act (2007)

Employment contracts ought to be well-tailored to fit the specific demands of the job at hand, and with due regard to the provisions of the Employment Act. Typically, a basic employment contract should cover the terms and conditions of employment, while outlining the duties and responsibilities of the employee.

Depending on the scope of engagement, an employer might need to incorporate well drafted non-disclosure, non-solicitation and non-compete clauses into the employment contract. The three *'Nons'* are particularly important for employers who deal with proprietary, confidential and sensitive information, have valuable or sensitive customer/client lists, or work in a highly competitive marketplace. These are a must-have for such employers and may either be included in their standard employment contracts or stand-alone agreements.

Employment policy manuals are also important in setting policies in place that make the workplace environment conducive for all parties and outline procedures to be followed in various processes. Employers should take advantage of these to further limit exposure to liability.

Sexual harassment at the work place and the rise of constructive dismissal as a remedy for employees

Just what constitutes sexual harassment? According to Paludi Michele Antoinette, Sexual harassment is described as a range of actions involving the harassment of a person due to his/her sex.

In Kenya, most employers are found liable for sexual harassment not necessarily because the act of sexual harassment occurred, but rather for failure to have a sexual harassment policy in place as required by the law. Section 6 (2) of the Employment Act, 2007 requires an employer to have such policy in place. Courts have found that failure to comply could result to liability.

From statistics, cases of sexual harassment mostly arise amid claims of unfair termination. This happens where the terminated employee cries foul and institutes claims against the employer for allegedly soliciting sexual favours and terminating them unfairly for not succumbing to the said advances.

What, on the other hand, is *constructive dismissal?* Constructive dismissal may be understood as a cessation of work because continued employment is rendered impossible, unreasonable or unlikely. For instance, when there is a demotion in rank or diminution in pay or both constructive dismissal will be found to have taken place. Similarly, it arises when a clear discrimination, insensibility, or disdain by an employer becomes unbearable to the employee. The

Constructive dismissal is essentially a forced resignation by dint of intolerable working conditions.

Employers should particularly note the following as the main triggers for employment disputes: termination/dismissal; breach of employment contract; injury at work; sexual harassment; discrimination; waiver of claims; service pay and conflicts with trade unions.

test of constructive dismissal is whether a reasonable person in the employee's position would have felt compelled to give up their job under the circumstances.

Constructive dismissal is essentially a forced resignation by dint of intolerable working conditions. In such situations, the employee is entitled to resign and yet claim damages from the employer as though he had been unlawfully dismissed. In Kenya, the Employment and Labor Relations Court adopted this doctrine in the case of *Coca-Cola East Central Africa Limited V. Maria Kagai Ligaga (2015) eKLR.* The Court reasoned that an employee is entitled to leave when the employer's behaviour towards the employee is so unreasonable that the employee cannot be expected to stay. The employer's conduct must be so grave that it constitutes a repudiation of the contract of employment. The breach must go to the very root of the contract. In other words, the employer must have breached the terms of the employment contract in such a manner that it is no longer possible for the employee to continue working effectively.

Noteworthy, the employee must however exercise this right of constructive dismissal at the earliest instance of noting breach in the employer´s conduct. Continuance to work under the breach may be construed as a ratification of the breach.

Way forward for employers

The importance of fostering healthy employment relationships cannot be overstated as they translate to great tasks management and performance at the workplace. Employers must watch out for potential pitfalls to stay compliant and avoid expenses incurred in defending claims lodged in court.

Employers should particularly note the following as the main triggers for employment disputes: termination/dismissal; breach of employment contract; injury at work; sexual harassment; discrimination; waiver of claims; service pay and conflicts with trade unions. Employers must avoid these pitfalls by following the stipulated procedures in the various laws.

One such way is to develop internal human resource policies to address these potential landmines in line with Section 6 (2) of the Employment Act, 2007. The policies should be both proactive and reactive as it would serve as an indemnity to the employer. As the old adage goes: prevention is better than cure.

For more information on this,
contact John M. Ohaga
johaga@tripleoklaw.com

Digitization of Land Records

Janet Othero
Cheptoo Langat

Previously, the Ministry of Lands has relied on a paper-based system to discharge its mandate. This system has proved untenable in this era of great technological advancement. The Ministry of Lands commenced a digitization exercise a couple of years ago which included scanning all lands office records. This is a project spearheaded by various ministries of the government to improve the efficiency of its services and operations by enhancing transparency in the system. As for digitization of the lands records, the main objective is to reduce the number of disputes pertaining to land and ease operations at the said office.

The digitization process has presented some discrepancies with existing law, that is the bulk of the content of a case lodged in court by the Law Society of Kenya. The suit seeks to quash a publication by the Ministry of Lands in the Daily Nation on the 4th April 2018, stating that land transactions will be processed online with effect from 13th April 2018. The orders sought in the suit amongst others, were to compel the Ministry of Lands to set up a consultative task force for the creation of electronic registration and conveyancing. This will be considered against the background of the proposed Land Registration (General) Regulations of November 2017 that were recently passed in Parliament.

This article does not seek to analyze the merits and demerits of case.

Challenges

The Land Act and Land Registration Act of 2012 were enacted with provisions requiring the National Land Commission and Ministry of Lands to come up with standardized conveyance forms and registration regimes. Parliament recently gazzetted the Land Registration (General) Regulations to give effect to electronic filing of registrable land documents. Of importance to note is that the regulations are subsidiary to the legislation in place and are mainly procedural. In its provisions relating to electronic registration and conveyancing, it does state that all dealings under the enabling Act shall be carried out in electronic form.

The Advocates Act at Section 34 stipulates that no unqualified person shall take instructions to draw or prepare any document or instrument relating to the conveyancing of property. The regulations appear to secure the role of advocates by providing standard forms that require attestation of advocates where required. The regulations do state that the electronic system will be configured paying regard to provisions of the Advocates Act on the qualifications of persons who may draw and engross conveyancing documents.

Currently, the Lands Information Management System (LIMS hereinafter) portal does not provide for an avenue for such inclusion of advocates to carry out transactions. It is configured in a way that any transactions have to be undertaken against a personal account of the parties to the transaction thereby removing advocates from the equation once documents are drafted. With the introduction of standard forms to the public, the role of advocates is further diminished from the process.

Moreover, the online portal contravenes Section 2 of the Stamp Duty Act as it purports to collect Stamp Duty whereas the Act states that it is the role of the Collector of Stamp Duty at the Kenya Revenue Authority (KRA hereinafter). The stamp duty is assessed under the LIMS portal and the stamp duty amounts are payable against a bank code or M-pesa paybill number issued under the same portal. These amounts are payable to a non-traditional KRA recipient account. It is also unclear how the payment of Stamp Duty and Capital Gains Tax will be done under the online system

Further, there are valid concerns raised that there was no public participation in the digitization process. This is evidenced by the various gaps in the system, with no information available such as how to process documents under the Government Land Act (Repealed), new leases, sub-

leases, extension of leases, change of user, letters of allotment and provisional certificate of titles. It also does not provide for simultaneous registration of documents such as discharge, transfer and charge. Further LIMS does not seem to consider the transfer and transmission of deceased person's property whose National ID cards and phone numbers have since been surrendered[1].

There have been complaints that while digitization seeks to make the conveyancing process secure and efficient, the online system has failed to achieve this in its initial launch. For instance, in conducting a search manually, the process would take less than a week to complete. Under LIMS, the time taken has not been ascertained for reasons including not all the files were scanned and uploaded in the system. Further, official search results under the RTA system contained the entire history of the land, while the search results procured using LIMS do not contain the entire history.

One of the most overlooked issues arising is the security and privacy of the records and data. While with the manual system there was a degree of safety in that only authorized personnel could access the lands records, stakeholders are yet to be advised on the security features of LIMS from local and international hackers. The government has outsourced this service from a third party. There is no clarity regarding which jurisdiction the data is housed and how the same can be accessed if the third party terminates its services with the government.

Kenyans place high value on land hence valid and accurate land records are very crucial. It is not in dispute that digitization is positive and could go a long way in improving the services offered by the Lands Registry.

Digitization of land transactions is expected to improve efficiency in the registries, fast and efficient retrieval of records and improved confidence of the public in the Ministry of Lands.

Recently, the cabinet secretary at the Ministry of Lands called for a stakeholders meeting to be attended by representatives of various professional bodies including the Law Society of Kenya. The objective is to ensure a smooth implementation in the digitization roll out. The role of advocates in the whole digitization process remains to be fully appreciated but a disruption in the traditional conveyance practice for most stakeholders is imminent and welcome.

For more information on this,
contact Janet Othero
jothero@tripleoklaw.com

[1] The minimum requirement to open an account with the E-Citizen online platform where LIMS is hosted is a valid phone number and national identity card. A verification code is sent to the mobile phone number and only one phone number can be registered against a user or national identity card.

Superior Service;

DO INVESTMENT BANKS OWE A FIDUCIARY DUTY?

Tom Onyango
Hilda Njoroge
Kivindyo Munyao

In recent years, Kenya has witnessed growth in various sectors such as finance, industry, real estate and technology amongst others. The growth of these sectors has spawned investment demand and consequentially increased investment service offerings in the country. Investment products have grown both in volume and complexity and are tailored for both novice and sophisticated investors.

The growth of investment opportunities in the country has seen the rise in demand for investment advice and services. Amongst the primary institutions providing investment advisory services are investment banks which like stock brokerage firms are primarily regulated by the Capital Markets Authority under the Capital Markets Authority(CMA) Act and the Capital Markets Authority Regulations of 2011.

The CMA Act defines an Investment Bank as a non-deposit taking institution licensed by the Capital Markets Authority to advise on offers of securities to the public or a section of the public, takeovers, mergers, acquisitions, corporate restructuring involving companies listed or quoted on a securities exchange, privatization of companies listed or to be listed on a securities exchange or underwriting of securities issued or to be issued to the public and to engage in the business of a stockbroker or dealer . The Act further defines an Investment Adviser as any person who, for remuneration carries on the business of advising others concerning securities or pursuant to a contract or arrangement with a client, undertakes on behalf of the client (whether on a discretionary authority granted by the client or otherwise), the management of a portfolio of securities for investment.

The demand for investment banking services is driven to an extent by the information asymmetry that exists between investment banks and their clients i.e.

> **The growth of investment opportunities in the country has seen the rise in demand for investment advice and services.**

potential investors and offerors or issuers of securities. Clients place trust and confidence in their investment bankers to act in their best interest. However, this informational asymmetry may inevitably breed situations that lead to conflict of interest and misaligned incentives. The multiple services offered by an investment bank and the multiple clients to whom these services are offered creates an environment where conflicts of interest are likely to occur. For example, an investment bank's self-interest in making money and generating business for itself may conflict with that of its client or the investment bank may find itself in a position where interests of one client conflict with those of another. In its engagement with a client, an investment bank will be privy to ideas, information and documents. Many disclosures that occur between the bank and its client may involve non-public and confidential information. Given the foregoing, the issue of the standard of care that investment banks should have towards their clients, beyond contractual duties, is a critical one.

The fiduciary obligation is an extremely demanding standard of propriety in conduct, and courts in regarding it, have not formulated a specific test to determine whether a relationship is fiduciary in nature or not; inquiry into the issue of fiduciary duty is highly fact sensitive. There are several established fiduciary relationships such as lawyer-client, trustee-beneficiary, agent-principal and director-shareholders of a company.

Although the CMA Act and its Regulations clearly provide for the formation, regulation and running of investment banks, the issue of fiduciary obligation is not mentioned. Furthermore, courts in Kenya have not established a legal position as to standard of care and fiduciary duty in relationships between investment banks and their clients.

Should a fiduciary duty arise in an Investment Bank-Customer relationship?

An investment bank holds itself out as an expert in the provision of its services, be it underwriting a specific security or managing a portfolio of securities for its clients. Furthermore, investment banks also offer financial advisory services. In view of such circumstances between an investment bank and its client, a reasonable expectation arises that an investment bank will act in its client's best interests for the purposes of the transaction.

The obligation to avoid positions of conflict prohibits a fiduciary from putting himself in a position where his duty conflicts with a duty owed to a third party or with self-interest. An imposition of a fiduciary obligation on investment banks to avoid conflicts of interest raises practical difficulties because the organizational nature of investments banks and the informational barriers present may increase the potential for conflicts to occur and may make them inevitable e.g. where the investment bank acts for both issuers as well as investors. In discharging a fiduciary duty, an investment bank may be required to decline instructions from a prospective client if likely to give rise to a conflict between the investment bank's duty to that client and either the investment bank's self-interest or its duty to another client.

It can be argued that in the context of offering financial advisory services, the relationship between an investment bank and its client is fiduciary in nature because the investment bank provides a specialist service to a client with the expectation that the client will rely on that advice. This issue of fiduciary duty in offering financial advisory services has been considered in different ways by courts in Australia, Singapore and the United Kingdom but has not been judicially interrogated in Kenya. The courts will likely examine all the aspects of the relationship, between the investment bank and its client, including the terms of any contract to see whether it was reasonable in the circumstance to expect the client to rely on the advice, and how far the client was susceptible to poor advice.

It is important to differentiate between misleading advice and advice that results in a loss for the client. Where an investment bank offers misleading advice to a client and the client relies on this information his detriment, then this could amount to fraud. But in a situation where an investment bank based on exhaustive research (noting how critically information underpins the market) verily believes that a security might do well based on its interpretation of the market, then it is irrelevant that the client suffers a loss because the investment bank has provided sufficient information for the investors to evaluate the security within their own interpretation of the market.

While the issue of the fiduciary obligation has not been well established by courts in Kenya, it is important that investment banks and their clients reflect on how the same would be determined considering the aspects of trust and confidence that underpins their relationship and its potential social utility. It is however difficult to ascertain how the courts would determine the same due the fact sensitive nature of such a determination.

While the issue of the fiduciary obligation has not been well established by courts in Kenya, it is important that investment banks and their clients reflect on how the same would be determined considering the aspects of trust and confidence that underpin their relationship and its potential social utility.

While investment banks in providing their services may encounter situations of conflict of interests, in the absence of a judicial determination on the fiduciary obligations, it is imperative to consider the language used in the engagement contracts between investment banks and their clients. Are these engagement contracts drafted to modify or exclude fiduciary liability or should they be drafted with fiduciary standards in mind? Further in the engagement between an investment bank and its client, it is also important to reflect on how and whether the regulatory regime promotes or bolsters standards that are fiduciary in nature

Given the foregoing, it will be of interest to see how Kenyan courts address the issue of fiduciary obligation of investment banks when called upon to determine the same.

For more information on this,
contact Tom Onyango
tonyango@tripleoklaw.com

John Ohaga and winning students from Strathmore University at the TripleOKLaw sponsored China Africa Joint Arbitration Center (CAJAC) conference in South Africa.

TripleOKLaw's Leyla and Mbula with former chair CIArb-Kenya Mr.Kariuki at the Inagural Women in Arbitration Conference in Nairobi.

JMO-unbreakable bonds

John Ohaga and winning students from Strathmore University at the TripleOKLaw sponsored China Africa Joint Arbitration Center (CAJAC) conference in South Africa.

TRIPLEOKLAW - The Firm

Front Office-Service with a smile

TOK-Always Wakanda ready

TOK-We trust each other to never walk alone

TOK-We listen, understand and then act!

JKK-How we are always ready to catch those briefs

TRIPLEOKLAW
ADVOCATES

EMPLOYEES OF THE QUARTER

Bernard Ngunzi
FINANCE MANAGER

Winnie Ayimba
ASSOCIATE – BANKING & REAL ESTATE

Rose Jerotich Agega
PERSONAL ASSISTANT

Practice Areas

ALTERNATIVE DISPUTE RESOLUTION

This Team is dedicated to the Alternative Dispute Resolution (ADR) practice. Our aim is to always offer business solutions customized to our clients' interest. We understand the importance of settling disputes where possible before formal proceedings are commenced

Contact person: johaga@tripleoklaw.com

CORPORATE AND COMMERCIAL

We advise corporates, listed companies and financial institutions on the various regulatory requirements for businesses in various sector specific regulations considering the dynamic legal and regulatory framework.

Contact person: jkibet@tripleoklaw.com

FINANCIAL SERVICES

Our Financial Services team of advocates support individual and corporate clients, financial institutions and SMEs in undertaking various investment projects in liaison with other professionals in the financial services sector. We provide wealth management services, project management and finance, environmental scanning for projects among others.

Contact person: dkagagi@tripleoklaw.com

BANKING AND REAL ESTATE

We handle a substantial amount of banking and real estate transactions. The practice area has grown rapidly in tandem with disruptive technologies and the real estate sector in Kenya. The firm handles transactions relating to property acquisition and disposal, due diligence on property, bank securitization and financing arrangements.

Contact person: tonyango@tripleoklaw.com

DISPUTE RESOLUTION

We have a team of experienced Advocates who have handled numerous landmark cases over the years and contributed immensely to the development of jurisprudence in Kenya. Over time we have a proven track record of excellence and diligence, providing timely legal service and support to our clients in various sectors.

Contact person: jochieng@tripleoklaw.com

TELECOMMUNICATIONS, MEDIA AND TECHNOLOGY

The firm has a practice area dedicated to Telecommunications, Media and Technology. As organizations continue to digitize their operations, we offer innovative legal solutions that not only ensures compliance but also mitigates exposure to associated risk.

Contact person: ckariuki@tripleoklaw.com