# Examining "Electronic Fraud" in Kenya and the Impact on Commercial Justice

***The Author: Dr. Peter Onyango Onyoyo (PhD)***[1]

***ABSTRACT:*** *Postmodern time has transformed the world status of affairs in doing business, perceiving and conceiving law in society today. One of the key challenges is the strategic shift from the use of analogue to digital means of transacting business. It is a fact that business behaviour has evolved from man in the cave to man of the computer rendering the world order more efficient. The more we appreciate technology and historic scientific discoveries the more we get into various challenges. New media have brought along new crimes such as, cybercrimes, internet, or computer crimes. Now that many people are hyper-connected in cyberspace, a reality that is becoming increasingly busier, people are interacting freely in carrying out their affairs online. Use of computer is no longer a privilege for the elite who gather to disseminate information but an open space for doing real business. Consequently, this comes with a price to pay, namely, new financial offences such as online fraud. The author is interested in exploring how e-commerce is changing behaviour of business in Kenya today. The discussant is pre-empting legal implications of the e-commerce and how law and policy makers should promptly respond.*

***Keywords****: Cybercrime law, biometric systems, e-security, e-finance, e-banking, i-tax, commercial law, Frauds, State responsibility to offer financial security.*

## Table of Contents



[1] The writer is a lecturer, School of Law, University of Nairobi, Kisumu Campus. The Research is meant for law students, researchers, and practitioners.

# INTRODUCTION

> *Over the last decade technological advances have been revolutionizing the conduct of commerce and financial transactions. Technology has allowed financial services to be provided to a wider variety of institutional and retail clients at far lower transaction costs, with important implications for access to financial services. The advent of the Internet and advances in cellular, wireless, and satellite technology have multiplied the possibilities for moving digital information. Many emerging markets are aggressively adopting advanced technologies in efforts to bridge the "digital divide."*(Fatima 2011).

President Obama said during his inaugural speech, "For the world has changed, and we must change with it"(Woodward 2014). As much as the law holds to its traditional tenets seeking, thereto, to maintain its own logics, the revolution caused by information and communication technology cannot be wished away.(Creech 2013). We are living in a hyper-connected world where machines have taken over most of the mathematical queries the modern time has been at pain to resolve. Technological advances have revolutionized business associations making business transactions simpler, faster, easier, and comfortable than ever before in human history.

Paradoxically, the same electronic or digital revolution is revealing some serious legal challenges in the sector of security, privacy, and freedom of expression, especially in the emerging economies including Kenya.(Fatima 2011).

The Republic of Kenya (EAK) is one of the East African countries whose economy is rapidly revamping itself in order to suit the new requirements of digital technology. With the introduction of M-Pesa by Safaricom in 2007, banks realised that more money is circulating in the mobile telephony network than the ordinary banking networks creating conflict of interests and competition. In this case traditional banks are compelled to re-invent their policies which should accommodate electronic systems including e-banking as a mechanism to counter-stand their competitors namely, the telecommunication companies.

> *The Communications Authority of Kenya (CAK) has cleared Equity Bank to start operations of its mobile phone and cash transfer service before it resolves a petition filed by leading telecommunications provider Safaricom, which is opposed to the bank using ultra-thin SIM cards* ('Equity Bank Cleared to Launch MVNO Normal SIM Cards' 2014).

It is a fact that mobile banking through telecommunication means is an innovative system attracting major concerns of banks especially for its potential profitability. Given that, much more money is circulating on the M-Pesa and many bank users have reduced their use of conventional banking systems, the conflict of interest is another evident legal battle to admit.

> *A mobile virtual network operator (MVNO) is a wireless communications services provider that does not own the wireless network infrastructure over which it provides services to its customers. An MVNO enters into a business agreement with amobile network operator to obtain bulk access to network services at wholesale rates, then sets retail prices independently.* See more at: http://www.startupacademy.co.ke/blog/heres-how-equity-banks-mobile-venture-will-work/#sthash.l1Ryg6Zu.dpuf ('Here's How Equity Bank's Mobile Venture Will Work | StartupAcademy' 2014).

## BACKGROUND

That Kenya is swayed to join the machine controlled and automated economies, in terms of computer, internet, and new media, it is not strange to analyse the crimes and serious collateral damages coming along with hyper-connected era. Cybercrimes or computer crimes are in the increase in Kenya. Fraudsters from outside and from within Kenya get easy access to the system with impunity. There have been several cases in Kenyan Courts related to cyber-crimes: a Russian foreigner caught with several ATM (*A Russian man was arrested while trying to withdraw money using fake credit cards here in Nairobi. Security guards raised the alarm when they noticed the man slotting different cards in the ATM dispensers along Kimathi Street and drawing cash. (Automated Teller Machines*) cards('▸ Cash Thief Nabbed with More than 100 ATM Cards - YouTube' 2014), 77 Chinese nationals found with private cyber command centre in Runda Estate in Nairobi (France-Presse 2014) that can infiltrate banking system.

As much as Kenyan consumer behaviour is rapidly tending towards postmodernity and deploying digital machines to control transfer of money, any reasonable person must admit that internet offenses are there to stay unless the Government designs reticent financial legal frameworks to countermeasure fraudulent behaviour in the financial sector.

Cases of hackers are outgrowing normal fraud cases brought before courts. ID theft (Biometric Fingerprint Scan)(Fatima 2011), advanced electronic signatures (*"advanced electronic signature" means an electronic signature which meets all the following requirements (a) is uniquely linked to the signatory; (b) is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change to the data is detectable*); (Generation of Digital Signatures), data transfer, copyrights, trade-marks, patents, (IP), and getting into international and national banking systems is becoming an urgent research interest both for legal researchers and lawyers.(Fatima 2011).

Civil case number 756 of 2012 in the High Court of Kenya in Nairobi, a case Faulu Kenya Microfinance Taking versus Safaricom Limited shows:

> *The Plaintiff submitted, as regards its claim against the Defendant, that it had infringed on its copyrights in that the Plaintiff had proposed the same to the Defendant when seeking a joint venture with it, utilising the Defendant's mobile telephony platform.*

Mobile Phone Telephony Network especially concerning the business of M-Pesa introduced and operated by the Safaricom Limited, is another electronic banking system that has changed the Kenyan economy within few years. As much as it works for the low, medium and high economy, it comes with its own *sui generis* offences that likewise deserve legal investigation.

What M-Pesa started in a simple format in less than a decade has eventually become a general finance principle guiding the micro-economy and macro-economy not only in Kenya but almost within East African region. Users of mobile banking system have increased rapidly. Use of mobile phones, i-pad and tablets, and personal computer in transacting business has gotten into the ordinary economic DNA of the Kenyan society or social engineering stage.

> *M-PESA fraud seems to be following the same paths. The initial phase of M-PESA fraud has been purely sociological. Some examples of the sociological methods used include a fraudster sending a text message to an unsuspecting M-PESA customer – the message purporting to have originated from M-PESA – the sender then calls the victim and asks the victim to send back the money as it was sent to a wrong number. The victim complies and thereby ending up losing money in the process.* - See more at: http://www.kachwanya.com/m-pesa-fraud/#sthash.X5KzUyud.dpuf ('M-PESA Fraud Reaches Social Engineering Stage' 2014)

Mobile phone is in the hands of almost every Kenyan. The use of such software has also been simplified to meet the needs of every person despite education level. Simultaneously, theft and fraud, through mobile banking have been in the increase to an extent of prejudicing the entire existing commercial law sector and most importantly, the entire financial justice system.

> *As alluded to above, M-PESA fraud seem to be maturing step by step following in the footsteps of email and network related frauds. If this be the case, then Safaricom has a reason to worry as soon consumers won't be targeted by calls or text messages but possibly by viruses, trojan horses, and related malware. Then, the fraudsters would be thinking of how to target M-PESA servers and transfer the billions of shillings to their respective bank accounts. - See more at: http://www.kachwanya.com/m-pesa-fraud/#sthash.X5KzUyud.dpuf* ('M-PESA Fraud Reaches Social Engineering Stage' 2014).

## PATENT LAW VIOLATION

The Copyright Act under section 26 of the Act reads:

> *Copyright in a literary, musical or artistic work or audio-visual work shall be the exclusive right to control the doing in Kenya of any of the following acts, namely the reproduction in any material form of the original work or its translation or adaptation, the distribution to the public of the work by way of sale, rental, lease, hire, loan, importation or similar arrangements, and the communication to the public and the broadcasting of the whole work or a substantial part thereof, either in its original form or in any form recognizably derived from the original.*

This proviso is concerned with the "literary works" but not digital software as alleged by the plaintiff.

Litigating patent rights is also getting increasingly complicated when the matter is already in public domain as in the trial of the Safaricom Limited Company as quoted. Non-Disclosure Agreement signed between two parties is insufficient to support a winning case as the law stands. "*The important point about the patent is not whether it was valid or invalid, but what it was that it disclosed, because, after the disclosure had been made by the appellants to the world, it was impossible for them to get an injunction restraining the respondents from disposing what was common knowledge. The secret, as a secret, had ceased to exist*."

The burden of proof of the infringement of the industrial property rights lies with the complainant who must prove beyond reasonable doubt that he had the copyright to the alleged offence. Even if the case law holds that the Court can make reference to binding Court Precedents even from other foreign jurisdictions, still Kenya must work harder on its own domestic cybercrime jurisprudence in order to guarantee more electronic security in the financial sector.

Fraud management system must be tightened to avoid the ulterior offences both by business institutions and the government ('Safaricom Tightens Security on M-Pesa with Fraud Management System' 2014). Commercial mobile money transfer system requires tight regulations from the government. Kenya has outgrown ICT sector and social media has come of age. The Ministry of Communication has a great role to place in order to ensure sanity in the sector.

## DIGITAL TECHNOLOGY

> *The potential for digital advertising fraud exists anywhere that media spending is significant and performance metrics are ambiguous or incomplete. Nefarious groups have found ways to profit by infiltrating legitimate systems and generating false ad views, ad clicks, and site visits using robotic programs.*('Slide 1 - IABDigitalSimplifiedUnderstandingOnlineTrafficFraud.pdf' 2014)

Internet comes originally from the intranet which was meant for few persons connected to a computer within a small location such as a defined work place. However, the internet has now grown into a global connection and communication that traverses ordinary State borders, or rather, into what is called online traffic fraud. The new media mean that the globe is now

in serious business and online networking that engages millions of people around the globe in transacting business (Creech 2013). It is likewise necessary to consider electronic contracts and digital signatures and how such legal tools can be held authentic and binding at law.

> *The Internet was designed as an open network distributed system to ensure the survival of information. It was not originally designed to handle commercial and financial transactions. Yet, a mere decade after its widespread introduction into society, open network technology has increasingly become the primary tool by which governments, business and individuals all over the world are exchanging information.*(Fatima 2011)

Computer is a tool-box using complicated software which is interpreted by data processors and works more-or-less as the human conscience using stored memory. Developers of the foresaid software namely, e-banking and mobile money *inter alia*, work on digital technologies that process, store and transfer signals around the globe with limited restrictions both from international and municipal laws.

The foresaid electronic technology has rendered life much easier but more insecure than ever before. Unquestionably State agencies are rapidly adopting computing systems and use of e-learning to improve on bureaucracy and spur economic growth. The current bureaucracy is undoubtedly depending on digital technology for its survival and effectiveness. What is worrying is its consistency with the financial justice.

Cybercrime has added another vocabulary to the Blackstone's Law Dictionary showing that there is rapid transformation in the legal system (Berman and Reid 1996) world-wide. However, such emerging crimes still lack proper legislative and judicial interpretations not only in Kenya but by extension, in the world legal spectrum. The anatomy of such emerging digital crimes is still new and requires advanced research on science, technology and law. New crimes shall require knew legal knowledge and proper legal framework suitable to govern cyber-space crimes without interfering with other rights.

> *Cybercrime noun a criminal offense on the Web, a criminal offense regarding the Internet, a violation of law on the Internet, an illegality committed with regard to the Internet, breach of law on the Internet, computer crime, contravention through the Web, corruption regarding Internet, criminal activity on the Internet, disrupting operations through malevolent programs on the Internet, electronic crime, Internet crime, sale of contraband on the Internet, stalking victims on the Internet, theft of*

*identify on the Internet and financial fraud in the internet.*(‘Cybercrime Convention’ 2014).

The use of computer to alter data, or gain unlawful use, access of computer or services falls within the definition of cybercrime or computer crime. However, versatility of the computer renders drawing lines between criminal and non-criminal behaviour regarding its use difficult (Smith, Grabosky, and Urbas 2004).

As things stand, cybercrime (crime on internet) is challenging judicial authorities to take necessary steps to develop tenable cybercrime jurisprudence. Such shall require a new legal doxology in terms of methods of teaching and communicating the law, a new Intellectual Property Jurisprudence, methods of drafting legislations, ways of interpreting and enforcing the law and new approach of delivering financial justice. Such need shall shake the traditional practice of commercial law and shift the minds of practitioners to an improved digital understanding of financial laws.

## REVOLUTIONIZING THE FINANCIAL LAW

*Because of the versatility of the computer, drawing lines between criminal and noncriminal behavior regarding its use can be difficult. Behavior that companies and governments regard as unwanted can range from simple pranks, such as making funny messages appear on a computer's screen, to financial or data manipulation producing millions of dollars in losses. Early prosecution of computer crime was infrequent and usually concerned Embezzlement, a crime punishable under existing laws. The advent of more unique forms of abuse, such as computer worms and viruses and widespread computer hacking, has posed new challenges for government and the courts* (‘Computer Crime’ 2014).

As Kenya is moving rapidly towards adopting new electronic system, some European countries are reluctant to adopt mobile banking into their systems due to some cynical minds regarding the technology. E-banking is one of the systems that some developed countries are treating with due precaution because of its vulnerability to manipulation of digital data.

The truth of the matter is pegged on *de facto* serious risks it may bring into the already fragile world financial status following the American economic depression in the capital economy.

Kenya is still a *de jure* novice when it comes to technically developed jurisprudence, particularly, in the ICT sector. The innovative understanding of how the whole electronic mechanism operates is still not a privilege *ad omnibus*. Many citizens still require legal empowerment and bold training on the use of digital technology including understanding how it can benefit the economy (domestic economy) without falling victims of financial cartels.

Evidentially, most of the software developers originate from emerging economies, namely, Asian region where, e-money, and financial market have been developed. This challenge should be the sufficient impetus for policy and law makers in Kenya to develop keen interest.

Predictably, if the same minds behind the digital technology, already unanimously adopted in the Kenyan financial regime, *mala volente* cyber criminals, decide to defraud the country of its hard earned wealth, then there will be no option other than succumbing to the unpleasant collateral effects of the ICT. Hackers are good at circumventing such innovative technologies to their favour as so long as they have economic and legal opportunities. Such fraudsters who are simple persons but with brilliant knowhow, and innovative minds, can possibly infiltrate into the financial system whenever there are loopholes in the legal system.

Laws governing financial justice ought to be reviewed by Parliament. New banking laws must contemplate areas of online fraud. There is need for anti-cybercrime regulations such as Espionage Bill, improved anti-trust Bill, Cybercrime Bill, and other laws related to the new crimes brought about by the digital technology.

## THE LEGISLATION

The Constitution of Kenya (‘Kenya Law: The Constitution of Kenya’ 2014) has been referred to as progressive Constitution which seeks to revolutionize a nation whose independence is barely 5 decades ago. Such progress entrenched in the constitution includes Bill of Rights and Service delivery clauses. The new dispensation puts Kenya at a high-tech level that will require legislative onslaught on the existing financial laws. Such laws must be compatible with the spirit and letter of the Constitution and lead the whole nation to the desired progress.

Legislators are expected to be men and women informed about the postmodern time and machine culture. It may not work if the legislators of the old school of thought are still the ones to craft financial laws. At this level Kenyan system (Electoral Act) puts an education threshold on State officers including politicians but does not specify in which discipline. Such

loophole has seen some astute politicians faking degrees, bribing universities or acquiring such degrees in dubious means.

The Constitution of 2010 and its provisions have changed the attitude towards politics. Same legislators of the 10th Parliament watered down the integrity clauses and the tendency has been to lower the degree requirement. However, faking university papers or irregularly acquiring such papers has become the best alternative for some individuals.

It is the mandate of the legislature to make, un-make and amend laws. Cybercrime law is a need whose time is running out with time. Kenya now needs a proper legislation to address cybercrimes especially concerning financial offences.

Cybercrime Prevention Act of 2012 in Philippines is an effort towards the right direction despite other legal challenges ('Republic Act No. 10175 | Official Gazette of the Republic of the Philippines' 2014). Kenya is of age to enact anti-crimes law. It may require time but time is now. It would be ideal to introduce financial police to carry out vigilance on any financial malpractice in Kenya.

## THE EXECUTIVE

The Executive is the Government in whose docket law enforcement and policy drafting resides. The same organ has its power shared with Parliament and the Judiciary when it comes to the e-security. But still the new Kenyan Government is under pressure to implement the Constitution and see Kenya achieving its vision 2030 without disappointments. This can only be done if the same Government deploys smart minds in the ICT sector to spur its economy.

The recruitment and appointment of the Cabinet Secretaries and Principal Secretaries have been done through rigorous vetting process and interviews to avoid traditional way of awarding jobs to wrong persons. Nominated contenders are taken to the Executive for appointment which must be backed by Parliament. The due process holds that the President is under constitutional obligation to present such names to Parliament for approval before giving them the job.

Formulating e-security policy must balance a number of competing complex concerns and in this sense it is just one of the requirements for risk management strategy. For instance, the Government of Kenya has alleged ghost workers and the best way to track them down and mitigate such risks is by introducing new digital policies including biometric technology. It is in this direction that Government shall manage its explosive wage Bill and maintain law and order.

## THE JUDICIARY

The Judiciary is an independent body which is expected to interpret the law and enforce it without any political interference (observing impartiality principle). With the new dispensation the Judiciary also has undergone some drastic constitutional transforms including vetting of judges and magistrates. The Judicial Service Commission is charged with duty to ensure that the organ is adhering to the progress required for by the Constitution. The judicial officers must be men and women not only with integrity but also with professional acumen and technological knowhow to handle justice system.

The recruitment of judges, magistrates and other Court officers is not political and the rationale is to render the sector more professional. Despite the wrangles of power surrounding the three arms of Government the Judiciary maintains its independence and autonomy. However, still it relies on the other organs for its service delivery mandate. The Legislature must amend and enact new laws that will be compatible with the postmodern challenges such as e-banking, e-finance and e-fraud. The same legislature relies on the Executive to come up with policies and measures that shall ensure effective law enforcement frameworks and avail the funds to carry out the work needed in time.

## COMPLAINTS AND RESPONSES

Academics and practitioners both have concerns about the legal framework and financial security at the age of electronic revolution. The following questions require urgent answers:

How is Kenyan legal system prepared to handle international electronic fraud?

How are the Kenyan banking laws and other financial laws ready to handle electronic system failure, cybercrimes and other malaise that may come with the new technology?

Is Kenya preparing home grown minds to accommodate electronic technology with efficiency and expediency?

Does the Country have strong financial schemes and strategy to make it excel despite the world economic depressions?

Wage Bill has been a thunderbolt of the 4th Kenyan Government and tendency to deal with it is still remote and far fetching.

There is call to increase the borrowing rate which is now hitting the celling at 1.3 trillion. Kenya is heavily indebted to such States as China just to name few. Will the economy stand with stagnant domestic income pro capita?

As the middle class is scaling up in Kenya the number of those who live below poverty line is also increasing. How is the Country managing the gap between the rich and the poor?

Education system, the so called 844, is proving to fail the test of time and may require drastic overhaul or amendment. Generally corporate world discusses the quality of graduates from the Kenyan institutions. The education system requires major overhaul in order to deliver. What is the Government planning towards this?

The rate in which the Country is adopting electronic technology and adapting it to suit its needs is not in tandem with population preparedness. With time, predictably, Kenya will have to import more foreign expertise. Already foreign companies and experts are awarded State tenders under the Government auspices. How will this enable citizens to create employment and invigorate the stagnant economy?

## RESPONSE

Some of the above paramount questions may require directions in terms of answers. The research reveals that Kenya can still achieve its objectives and put its house in order if there is good will to do so. The country may not require the massive importation of ideas in terms of hiring Chinese companies to do some technical and professional jobs but can limit the amount of foreign companies and revamp the capacity of local companies (develop human resource).

> *Police find equipment capable of infiltrating bank accounts and cash machines in raids on homes in upmarket area of Nairobi Kenyan police have arrested 77 Chinese nationals on suspicion of running a cybercrime centre from homes in an upmarket area of the capital, Nairobi*(France-Presse 2014).

> *The Daily Nation newspaper said equipment capable of infiltrating bank accounts, Kenya's M-Pesa mobile banking system and cash machines were discovered after a series of raids. "The suspects are being interrogated to establish their mission in the country and what they wanted to do with the communication gadgets. They have been charged in court," said the director of Kenya's criminal investigation department, Ndegwa Muhoro*(France-Presse 2014).

Kenyan devolved Governments have developed tendency of hiring foreigners for big tenders. Most of such awarded jobs shall be paid in long-term instalments with accrued substantive interests. The main rationale behind this choice is on technology and finance. Such open door policy requires precautions due to the fact that cyber criminals can find their way as well into the countries digital system through deployment of foreigners to deal with national jobs.

E-security is already a fragile reality. Given concrete cases above there is no option but to write new laws to deal with emerging commercial crimes.

The big answer to the above questions is just to revolutionize legal system in Kenya and adjust it to the new requirements. Such adjustment must take into keen consideration the digital technology that is now dictating the economy such as e-banking, e-finance, and mobile banking using internet software and world-wide-webs. A tight security system must be put in place and tame the money laundering and frauds. Money transmitters and internet service providers must also comply with international measures when it comes to e-security regulations.

> *Securing the open network is first and foremost the responsibility of the service providers. Businesses need to understand the risks and responsibilities of providing services via these channels and seek continuous improvement in maintaining e-security. Technology is only a part of the solution; sound business principles such as responsibility, accountability, and trust are also essential to building infrastructure and a framework that can support e-business.*(Fatima 2011).

## CONCLUSION

With clear remark, Kenya has embraced change and progress in its Constitution. Such change requires some sacrifice and hard work especially in the legal transformation system. Use of machines in terms of computer to handle our economy is a reality that a State cannot do without. As has been discussed in this examination paper, it would be misleading to handle

financial fraud today as a normal issue. It is a serious issue that can yield into mega financial scandal.

Cybercrime or computer crime must be urgently addressed. Proper legislations must be put in place to deal with whatever outcome or unexpected surprises such as the already mentioned scandals.

The reason being, Kenya is also signatory to regional and international financial agreements that certainly impose their obligation and confer rights. Kenya is a signatory to many international trade treaties and such like investment contracts are protected by the International Trade Law among others. Given this scenario it would be misleading to deal with e-banking, e-money, and fraud is as national problem but international reality.

The judiciary must be prepared to understand in wholesale the challenges facing the existing justice system and make proper suggestions that would lead the country to solution.

Legal education institutions must as well consider urgently reviewing their curriculum and adjusting it to the new ICT framework.

The Government must also be vigilant of whatever gets into its jurisdiction and evaluate every technology before adopting it in wholesale. The *bona fide* e-banking can be tamed by stringent laws and policies in order to counter stand frauds.

Law-makers and policy makers must as well be taken through the new technology and the law in a way that enacted laws may be compatible with postmodern requirements. It is a question of how to deal with computer crimes expeditiously and on time.

***REFERENCE***


'▶ Cash Thief Nabbed with More than 100 ATM Cards - YouTube'. 2014. Accessed December 12. https://www.youtube.com/watch?v=3O_d2rG5YrI.

Berman, Harold J., and Charles J. Jr Reid. 1996. 'Transformation of English Legal Science: From Hale to Blackstone, The'. *Emory Law Journal* 45: 437.

'Computer Crime'. 2014. *TheFreeDictionary.com*. Accessed December 12. http://legal-dictionary.thefreedictionary.com/Computer+Crime.

Creech, Kenneth C. 2013. *Electronic Media Law and Regulation*. Routledge.

'Cybercrime Convention'. 2014. *TheFreeDictionary.com*. Accessed December 12. http://legal-dictionary.thefreedictionary.com/Cybercrime+Convention.

'Equity Bank Cleared to Launch MVNO Normal SIM Cards'. 2014. *HumanIPO*. Accessed December 12. http://www.humanipo.com/news/46355/equity-bank-cleared-to-launch-mvno-normal-sim-cards/.

Fatima, Amtul. 2011. ‘E-Banking Security issues–Is There a Solution in Biometrics’. *Journal of Internet Banking and Commerce* 16 (2): 2011–08.

France-Presse, Agence. 2014. ‘Kenya Arrests 77 Chinese Nationals in Cybercrime Raids’. *The Guardian*, December 5, sec. World news. http://www.theguardian.com/world/2014/dec/05/kenya-chinese-nationals-cybercrime-nairobi.

‘Here’s How Equity Bank’s Mobile Venture Will Work | StartupAcademy’. 2014. Accessed December 12. http://www.startupacademy.co.ke/blog/heres-how-equity-banks-mobile-venture-will-work/.

‘Kenya Law: The Constitution of Kenya’. 2014. Accessed September 5. http://kenyalaw.org/kl/index.php?id=398.

‘M-PESA Fraud Reaches Social Engineering Stage’. 2014. *Kachwanya.com*. Accessed December 12. http://www.kachwanya.com/m-pesa-fraud/.

‘Republic Act No. 10175 | Official Gazette of the Republic of the Philippines’. 2014. Accessed December 12. http://www.gov.ph/2012/09/12/republic-act-no-10175/.

‘Safaricom Tightens Security on M-Pesa with Fraud Management System’. 2014. *HumanIPO*. Accessed December 12. http://www.humanipo.com/news/1341/safaricom-tightens-security-on-m-pesa-with-fraud-management-system/.

‘Slide 1 - IABDigitalSimplifiedUnderstandingOnlineTrafficFraud.pdf’. 2014. Accessed December 12. http://www.iab.net/media/file/IABDigitalSimplifiedUnderstandingOnlineTrafficFraud.pdf.

Smith, Russell G., Peter Grabosky, and Gregor Urbas. 2004. *Cyber Criminals on Trial*. Cambridge: Cambridge University Press. http://ebooks.cambridge.org/ebook.jsf?bid=CBO9780511481604.

Woodward, Paul. 2014. ‘“For the World Has Changed, and We Must Change with It.”’ *War in Context*. Accessed December 12. http://warincontext.org/2010/05/20/for-the-world-has-changed-and-we-must-change-with-it/.