REPORT ON CYBER-IDENTITY THEFT IN KENYA

1. Introduction

As information and computer technology (ICT) advances rapidly and more individuals and organizations embrace it more, cyber-crimes continue to pose a persistent challenge to the society (Zhang, et al., 2012).

Cyber-crimes refer to criminal activities that are either cyber-dependent (rely on Information and Communications Technology (ICT) devices as both the means and the target of the crime) e.g., hacking or creating and spreading malwares or cyber-enabled (traditional crimes that are expanded in scope or impact by the use of technology, computers, computer networks, or other ICT tools) e.g. fraud (Legal Guidance, 2019).

According to (PwC, 2020) report, cyber-crime in Africa ranks amongst the top areas of concern with 38% of CEOs citing it as a threat.

This report will centre its focus on one of the cyber-crimes, which is identity theft, and examine its various aspects within the context of Kenya.

2. Cyber-Identity Theft Manifestation in Kenya

Cyber-identity theft is the practice of using ICT or electronics means (e.g., via the internet) to gain unauthorized acquisition of personal identifiable information such as: full names, Identification numbers, addresses, sensitive documents, bank account information, etc., - with the intention of committing any form of deceitful or illegal activity, either online or offline (Close, et al., 2006).

For several years, identity theft has raised serious concerns globally and its cases have continued to sky-rocket due to an expanded range of identity theft methods (National council on identity theft protection, N.D.)

The January 2021 report from the Communications Authority of Kenya (CA) indicate that due to Covid-19 pandemic, there was a 159.9% rise in cyber threats from July-September 2020 as compared to the preceding three months, whereby, out of the 35.1 million recorded incidents, 27.4% were associated with online fraud Covid-19 pandemic (Money254 Team, 2021).

2.1 Types of Cyber Identity Theft

(Hussain & Cheng, 2022) lists several types of identity theft, such as:

- Financial identity theft: According to a study by Myriad Connect firm, fraudsters target digital and mobile money service transaction thus seven out of ten Kenyans have fallen victim to this (Sunday, 2019). For instance, (Otieno, 2022) reported how Mr Mugo fell a victim to this, whereby his stolen ID was used in KES 2.7m mobile money transaction.
- Medical Identity Theft: The victim's identity is used to obtain free medical care or benefits.
- Synthetic identity theft: the perpetrator uses both the stolen identity and fake information so as to create a new identity thus allowing them to make frauds.

- Child identity theft: Since a child has not build up information about themselves, they become more vulnerable to their identities getting stolen by the perpetrators and used for their own personal gain.
- Tax identity theft: the victim's personal information is used to file a false state or federal tax return to collect a refund.
- Criminal identity theft: a criminal falsifies his/her identity during an arrest so as to avoid summons or an arrest or a conviction.
- Business identity theft: performing illegal activities like fraud, by using the name of a business

2.2 Common Methods and Techniques

(Tajpour, et al., 2013) study identifies the various Identity theft methods. Some of these methods include:

- Eavesdropping on individuals giving out personal information or observing their activities at ATMs or while filling out forms.
- Skimming: Illegally attaching data storage devices to record ATM card or PIN numbers during transactions at ATMs or retail checkout terminals.
- Exploitation of publicly available information from public and government databases, private databases, social medias, etc.
- Old-fashioned Stealing and misplacing of sensitive documents:
- Retail theft and service providers selling the victim's information to organised criminals (Ndemo, 2019) .

- Spoofing and phishing: Sending messages and emails from a source pretending to be a trusted IP address, websites or institutions.
- Botnets and SQL Injection Attacks, whereby in 2015, a Kenyan in Nairobi was arrested and charged with violating Section 84 (B) (b) of the Kenya Information and Communications Act because he interfered with Safaricom's billing system, resulting to Sh3.6 million loses (Kahongeh, 2022).
- Social Engineering: Manipulating individuals through techniques like pretexting, phishing, vishing, smishing, typo squatting, etc, to obtain confidential information or prompt specific actions.

2.3 Transnational Impact of Cyber-Identity Theft

The effects of cyber identity theft are not limited to a single country but can have widespread consequences that affect multiple nations. For instance, Kenya's tech hub is valued at over Sh120 billion, making it both the Silicon Savannah of the region and a centre for cybercrimes. Nairobi has been linked to notable global cyber frauds, including a case where phishers in the Kenyan capital caused a Sh56.8 million loss to Fairfax County in the US (Kahongeh, 2022).

These consequences involve: international cooperation, cross-border investigations, coordination among law enforcement agencies from different countries.

Collaborative efforts and information sharing between countries are essential

in combating these threats posed by cybercriminals operating across borders and exploiting vulnerabilities in international systems.

3. Rights And Ethics Considerations in Dealing with Cyber Identity Theft Crimes

3.1 Privacy and Data Protection Rights

- On 30th May 2018, the Computer Misuse and Cybercrimes Act of 2018 was enacted in Kenya to protect the Confidentiality, integrity and availability of computer systems and data (Anon, N.D.).
- On 25 November 2019, the Data Protection Act No. 24 of 2019 came to effect in Kenya and on 31st December 2021, The Data Protection (General) Regulations, 2021, The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021; and The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, followed (Wako, 2022).
- Appointment of the Office of the Data Commissioner on 16th November 2020 granted it the power under the Data Protection Act to impose administrative fines for failure to comply with the Data Protection Act (Wako, 2022).
- Kenya Information and Communications Act, No. 2 of 1998, aimed at promote the growth of the information and communications sector, as well as electronic commerce (Wako, 2022).

- Kenya Information and Communications (Consumer Protection) Regulations, 2010, enacted to protect consumers of ICT services and products (Wako, 2022).
- The central Bank of Kenya issued Cybersecurity Guidelines for Payment Service Providers, July 2019, that was meant to establish a secure cyberspace and combat cybercrime due to the rising cyberthreats targetting banks (Wako, 2022).

3.2 Ethical and Legal Considerations

Prior to implementing new technologies, it is crucial to ensure adherence to data privacy regulations and laws so as for the technology to be efficient, for instance, Kenya's implementation for unique digital identifiers (huduma number) for all its citizens, carried the risk of government overreach due to lack of special protection for children (Mutung'u, 2021).

4. Implications and Limitations of National Laws

So as to address cyber-identity theft, it is crucial for national laws to be effective. This section covers the legal frameworks in Kenya.

4.1 Criminalization of Cyber-Identity Theft

- Under the Data Protection Act, non-compliance to the Data Commissioner's orders is considered as an offence (Wako, 2022).
- Section 65 of the Data Protection Act grants all data subject victims the right to compensation from data processors or controllers (Wako, 2022).

- Obstructing the Data Commissioner during an investigation is punishable by a fine of up to KES 5 million (USD 50,000) or imprisonment for a maximum of two years, or both (Wako, 2022).
- The Data Protection Act mandates that all data processors and controllers must register with the Data Commissioner's office and are required to follow the data protection principles like following the right to data privacy, etc (Wako, 2022).

4.2 Apprehension and Prosecution Challenges

- Poor handling of evidence in the chain of command results to cases been dismissible in court (Kahongeh, 2022)
- Lack of proper and advanced tools needed by law enforcement agencies in identifying, apprehending, and successfully prosecuting cyber identity theft offenders and lack of training on how to use these tools (Kahongeh, 2022).
- Lack of sharing of information between jurisdictions or law enforcement makes it challenging to apprehend and prosecute the offenders (Kahongeh, 2022)

4.3 Prevention and Awareness Measures

- Awareness and training: Training not only better enhances employee awareness of policies and procedures, but it also promotes a stronger culture of fraud prevention and it is commendable how Kenyan organisations are keen to raise awareness (PwC, 2020).

- Reporting a crime: (Mari, 2018) states how Kenyans are urged to file a police report as well as report to the organisations concerned (bank, network service providers, etc) as soon as your information is compromised either by fraud, theft or losing documents, etc.
- Implementation of technology that combats identity theft, for instance, when banks pushing vendors to follow a 2-step verification process for card or money transactions (Kivuva, 2022).
- Conducting cybersecurity risk assessments.
- In 2019, the Statute Law (Miscellaneous Amendments) Act established the National Integrated Identity Management System (NIIMS), also known as *huduma namba.* Additionally, in 2020, Kenyan government implemented an advanced identity systems and digital identity (*huduma numba* card) enrolment exercise covering civil registry, national identification, passport, birth certificates etc (Mutung'u, 2021).

5. Investigative Tools and Digital Forensic Evidence

Digital forensics play a crucial role in cybercrime investigations. It involves gathering, analysing, and presenting digital evidence in judicial processes (Holt, et al., 2022). With the rise of cybercrime, digital forensics helps uncover the tactics used, trace the attack sources, and gather evidence (Harbawi & Varol, 2016). Specialists utilize various techniques, and work closely with law enforcement and stakeholders to ensure justice and protection of Kenya’s cybersecurity environment.

5.1 Challenges and Limitations in Acquiring Digital Evidence

- Due to different law enforcement agencies, jurisdictions and legal frameworks, sharing of information and evidence is limited therefore the criminals might not be held accountable and prosecuted (Kahongeh, 2022).
- So as to guard their reputations, victims fail to report the crimes or admit to been victimized (Karanja, 2017)
- Poor collection and handling of evidence, for instance, a case where Mutuku, who allegedly defrauded Safaricom, an Internet Service Provider company in Kenya), for 5 years. Mutuku challenged the authenticity of a WhatsApp communication presented as evidence in court. He contested its validity by pointing out that the phone used for the communication was not submitted as evidence, prompting him to file a Notice of Motion. He asserted that the trial magistrate made an error by unlawfully admitting electronic evidence (WhatsApp chats) in violation of Section 65 (8) and Section 106 (B) (2) of the Evidence Act. Thus, leading to its admissibility (Kahongeh, 2022).
- In the online environment, gathering of evidence might be challenging when the attacker uses technologies like encryption, VPNs, multiple fake identities, etc, to minimize detection from law enforcement (Holt, et al., 2022).
- Due to Kenya been a developing country with slow technological advancements, it faces challenges in keeping up with the rapid global growth of technology and the increasing complexity of cybercrime (Kahongeh, 2022).

- Minimal training, expertise, capacity and resources required for cybercrime investigations results to investigators struggling to build cases. Moreover, judges' lack of understanding to some of the cybercrime technologies further complicates the process, causing delays in the identification, investigation and prosecution of cybercriminals, and at times denying justice to the victims (Kahongeh, 2022).
- Run-time vs performance whereby most forensics tools have a slow performance and takes a lot of time to complete a process thus resulting to detrimental impacts on investigations (Harbawi & Varol, 2016).
- The high cost of investigating and prosecuting cybercrimes particularly in cases involving: multiple countries requiring international cooperation or dealing with multiple jurisdictions and legal frameworks (Kahongeh, 2022).

5.2 Cyber Incident Response and Collaboration

The Kenyan government formed the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) to ensure a safer online environment in Kenya. Other than this collaborative framework been established in compliance with the Kenya Information and Communications Act of 1998, it is also responsible for coordinating national cybersecurity activities and serves as the primary point of contact for cyber security matters in Kenya (Communications Authority of Kenya, N.D.).

5.3 Speculative Future Developments in Investigative Tools

Lack of data audit and analysis solution hinders the ability to effectively analyse and audit data, and conduct investigations. Due to this, the Office of the Data Protection Commissioner expressed a need for a forensic analysis tool to identify companies that violate the privacy of their users' personal data (Ambani, 2023).

6. Critical Evaluation of Victims, Harm, Perpetrators, and Social Perception

6.1 Psychological and Financial Impact on Victims

- TransUnion’s digital fraud solution performed a survey that shows how Kenyan banks lose over $121.49 million every year to fraudster through identity theft (Anyanzwa, 2021).
- For victims to resolve an identity theft issue, a lot of time is taken, and is costly. Additionally, the victims can be stressed, angry, feel helpless, betrayed, have mistrust issues and worst-case scenario, be suicidal (Copes, et al., 2010).

6.2 Vulnerable Groups and Social Inequality

- (Hussain & Cheng, 2022) mentions how children are more vulnerable to their identities getting stolen due to them not having a lot of information, and also deceased people, whereby most of the time is their relatives or friends who steal their identities.

- In 2019, Financial Sector Deepening Trust (FSD) performed a survey in Kenya revealing that Mobile-money users (like M-Pesa) faced more challenges and experienced more financial losses due to fraud than the users of regulated financial services (like banks and mobile banks) (Anyanzwa, 2021).
- Not only are large corporations frequently targeted, but also mid and small sized companies like saccos, are also vulnerable to attacks, whereby the threat landscape has significantly expanded for businesses during the pandemic (Kahongeh, 2022).
- Cyber-criminals mostly target areas or people with less knowledge on technologies example in developing countries, senior individuals, etc (Copes, et al., 2010).
- From the FTC's 2003 data, higher earning individuals in the 25-54 age group are at a higher risk to be identity theft targets (Copes, et al., 2010).

6.3 Profiling Cyber-Identity Theft Perpetrators

- According to this TransUnion's digital fraud solution survey, identity theft criminals target financial and telecommunication businesses because there is more gains (Anyanzwa, 2021).
- Persistence and resilience.
- Cyber-criminals have a high level of technical expertise and they are mostly knowledgeable and adaptable to new technologies.
- Most of perpetrators are in organized criminal networks.

6.4 Social Perception and Stigma

Blaming and shaming of victims enables them to not report the crime or not do anything about the situation ending up receiving more damages.

7. Recommendations for Addressing Cyber-Identity Theft in Kenya

- More awareness and training programs should be conducted more often to both individuals and organizations' staff members.
- To gain a competitive edge, Kenya should thrive to equip itself with the appropriate and advanced tools and technologies. Plus provide comprehensive training on how to utilize these tools so as to maximize their potential impact (Kahongeh, 2022).
- Awareness and implementation of technologies that help in combatting identity theft, and enforce data privacy (Wambugu, 2023), e.g., LifeLock by Norton (Anon, N.D.), etc.
- Kenya's High Court should implement a cybercrime division, whereby judges and prosecutors should have cybersecurity and cybercrime training so as to be able to tackle cyber affairs (Kahongeh, 2022).
- Due to Kenya's high increase of online interactions and transactions that resulted to a surge of cybercrime litigations, better technology practices should be implemented e.g., multi-factor and physical authentication, etc (Kahongeh, 2022).

8. Conclusion

Cyber-identity theft is a significant challenge in Kenya. International cooperation and comprehensive approaches are needed to combat these persistent cybercrimes.

National laws play a crucial role in protecting privacy, but challenges like poor evidence handling hinder investigations. Prevention measures, awareness programs and stronger investigative skills and practices are essential. Digital forensics faces resource limitations, and the impact on victims and social perceptions complicates matters.

To address cyber-identity theft, legal reforms, capacity building, and resilience to cyber threats are required in Kenya to ensure a safer digital environment.

References

Ambani, B., 2023. *Data chief seeks system to secure private details.* [Online]
Available at: https://nation.africa/kenya/business/data-chief-seeks-system-to-secure-private-details-4094746
[Accessed 23 May 2023].

Anon, N.D.. *LifeLock.* [Online]
Available at: https://lifelock.norton.com/#
[Accessed 20 May 2023].

Anon, N.D.. *The computer misuse and cybercrimes act.* [Online]
Available at: https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act/
[Accessed 21 May 2023].

Anyanzwa, J., 2021. *Kenya's financial services firms prime target for fraudsters.* [Online]
Available at: https://www.theeastafrican.co.ke/tea/business/kenya-identity-fraud-financial-services-industry-3441762
[Accessed 25 May 2023].

Close, A. G., Zinkhan, G. M. & Finney, Z. R., 2006. Cyber-Identity Theft. *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce,,* pp. 168-171.

Communications Authority of Kenya, N.D.. *The National KE-CIRT/CC.* [Online]
Available at: https://ke-cirt.go.ke/
[Accessed 29 April 2023].

Copes, H., Kerley, K. R., Huff, R. & Kane, J., 2010. Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice,* 38(5), pp. 1045-1052.

Harbawi, M. & Varol, A., 2016. The role of digital forensics in combating cybercrimes. *2016 4th International Symposium on Digital Forensic and Security (ISDFS),* pp. 138-142.

Holt, T. J., Bossler, A. M. & Seigfried-Spellar, K. C., 2022. *Cybercrime and Digital Forensics: An Introduction.* 3 ed. Oxon: Routledge.

Hussain, A. & Cheng, M., 2022. *What Is Identity Theft? Definition, Types, and Examples.* [Online]
Available at: https://www.investopedia.com/terms/i/identitytheft.asp
[Accessed 20 May 2023].

Kahongeh, J., 2022. *How legal loopholes are hurting Kenya's cybercrime fight.* [Online]
Available at: https://www.businessdailyafrica.com/bd/data-hub/how-legal-loopholes-are-hurting-kenyas-cybercrime-fight-3727058#:~:text=Legal%20and%20forensics%20experts%20now,the%20biggest%20setback%20for%20investigators.
[Accessed 29 April 2023].

Karanja, J., 2017. *Cybercrime Related Investigations in Kenya.* [Online]
Available at: https://www.researchgate.net/publication/331431758_Cybercrime_Related_Investigations_in_Kenya
[Accessed 29 April 2023].

Kivuva, E., 2022. *Two-step card payments pile pressure on vendors.* [Online]
Available at: https://nation.africa/kenya/business/two-step-card-payments-pile-pressure-on-vendors--3804556
[Accessed 20 May 2023].

Legal Guidance, 2019. *Cybercrime - prosecution guidance.* [Online]
Available at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
[Accessed 20 May 2023].

Mari, G., 2018. *Why you should be worried if your phone or ID was stolen and you did not file a police report.* [Online]
Available at: https://www.pulselive.co.ke/news/local/identity-theft-why-you-should-be-

worried-if-your-phone-or-id-was-stolen-and-you-did/524l4s9

[Accessed 20 May 2023].

Money254 Team, 2021. *Identity Theft Nightmare: Kenyans Are Losing Millions to Fraudsters.* [Online]

Available at: https://www.money254.co.ke/post/identity-theft-nightmare-kenyans-are-losing-millions-fraudsters#:~:text=The%20pandemic%20has%20only%20exacerbated,were%20linked%20to%20online%20fraud.

[Accessed 20 May 2023].

Mutung'u, G., 2021. *Digital Identity in Kenya.* [Online]

Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://researchictafrica.net/wp/wp-content/uploads/2021/11/Kenya_1.11.21.pdf

[Accessed 21 May 2023].

National council on identity theft protection, N.D.. *2023 Identity Theft Facts and Statistics.* [Online]

Available at: https://identitytheft.org/statistics/

[Accessed 20 May 2023].

Ndemo, B., 2019. *We must curb identity theft crisis or face the consequences of our inaction.* [Online]

Available at: https://nation.africa/kenya/blogs-opinion/blogs/dot9/ndemo/we-must-curb-

identity-theft-crisis-or-face-the-consequences-of-our-inaction-137432

[Accessed 20 May 2023].

Otieno, S., 2022. *Puzzle of stolen ID used in Sh2.7m M-pesa transaction.* [Online]

Available at: https://nation.africa/kenya/news/puzzle-of-stolen-id-used-in-sh2-7m-m-pesa-transaction-3820176

[Accessed 21 May 2023].

PwC, 2020. *PwC Kenya Economic Crime and Fraud Survey,* Nairobi: PwC.

Sunday, F., 2019. *Phone users losing millions through identity theft.* [Online]

Available at: https://www.standardmedia.co.ke/business/article/2001287820/how-kenyans-lose-millions-through-mobile-phones

[Accessed 20 May 2023].

Tajpour, A., Ibrahim, S. & Zamani, M., 2013. *Identity Theft Methods and Fraud Type.* [Online]

Available at: https://www.researchgate.net/publication/273259976_Identity_Theft_and_Fraud_Type

[Accessed 20 May 2023].

Wako, J., 2022. *Data Protection and Cybersecurity Laws in Kenya.* [Online]

Available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya

[Accessed 21 May 2023].

Wambugu, S., 2023. *Our data is our life — please protect it.* [Online]

Available at: https://nation.africa/kenya/blogs-opinion/opinion/our-data-is-our-life-please-

protect-it-4111748

[Accessed 24 May 2023].

Zhang, Y. et al., 2012. A survey of cyber crimes. *Security and Communication Network,* Volume 5, pp. 422-437.