The GLOCEPS
Weekly Influential Brief
Research and Analysis in Transnational Organised Crimes

Gaps in preventing digital fraud in Kenya's financial systems

Ida Gathoni
Valtino Omolo

Photo Credit: stirworld.com

Executive Summary

This brief examines the gaps in preventing digital fraud in Kenya's financial systems and services. It explores cybercrime awareness amongst finance-based professionals and consumers; investigative and legal expertise; unregulated financial technology; and lastly institutional security systems. Suggested recommendations include, creation of public awareness on perpetration of digital financial crimes; enhancement of legal and investigative capabilities of relevant officials; improving monitoring systems within fin-tech institutions, and, lastly strengthening of security systems in financial institutions.

Context

By 2021, Kenya's financial sector establishments had been classified amongst the world's top targeted and preyed upon institutions by tech-savvy criminal groups. This classification was primarily attributed to inexpensive and easily accessible fin-tech products/services coupled with the country's surging mobile penetration rates. Subsequently, in 2022, hacking attacks targeting fiscal establishments were reported to have arisen nearly threefold, as the number of mobile subscriptions surpassed the country's total population by 12%. An estimated 444 million hacking incidents on the country's financial systems were reported by the end of June 2022 thus showing the high vulnerability of Kenya's financial systems.

The country's highly digitized economy, widespread internet accessibility together with weak security systems continue to catalyze financial systems' susceptibility to organized criminal groups. Digital financial services and products, particularly M-PESA and credit cards, continue to emerge as the new fraud frontiers within the systems. For instance, in 2017, victims of credit card fraud were estimated to have lost approximately KES 18 billion. The figure represents a 30% rise in lost revenue compared to 2016 pointing to the lack of effective strategies to curb online fraud within the country's financial sector. Separately, fin-techs also face challenges related to law enforcement and policing through money laundering schemes further accelerating financial crimes linked to foreign and local organized criminal groups.

Photo credit: Economic times

Key Issues

This brief addresses weaknesses in Kenya's financial systems that permit exposure to increased digital fraud.

Cybercrime awareness

Lack of comprehensive awareness on emerging cybercrime trends amongst professionals and consumers of financial services within the industry has led to an upsurge in online fraud. Such shortfalls continue to mount due to increased sophistication of fraudsters. The sophistication of organized crimes targeting self-service cash machines such as ATMs has been on the rise due to low financial awareness amongst many bank users. Additionally, a significant number of IT and security professionals are not aware of provisions as per the Data Protection Act, 2019. This indicates a gap in consumer initiatives within financial systems aimed at spreading awareness of emergent risks posed by organized criminal groups (OCGs). Equally a large percentage of fiscal institutions have insufficient awareness on corporate protective procedures against digital crimes, thus, increasing vulnerabilities of such establishments to fraudulent activities tied to OCGs.

There is also lack of understanding and insufficient familiarity with terms and concepts on digital financial crimes, specifically amongst judicial officials and court users. This continues to undermine the administration of justice. Such loopholes have led to the inadmissibility of evidence in courts thus resulting into low prosecution rates linked to financial crimes.

Investigative and legal expertise

Legal suits in Kenya against cybercriminals have risen over the years with only a few ending up in convictions due to inefficient legal and investigative technical expertise. Forensic and legal experts point to lack of tools, capacity and technical proficiency as key elements contributing to inadmissibility of evidence in courts. In turn, this leads to increased out-of-court settlements involving companies'/ business owners who opt to negotiate with cybercriminals' on ransom demands due to present difficulties in securing convictions for such crimes.

Further, the evolution of digital fraud in Kenya over the years continues to pose challenges to the country's legal professionals. Lack of prerequisites for online connections, new technologies like cloud storage and the Internet of Things, together with the growth of the dark web, continually offer latitude to cyber criminals through use of hidden identities, thus presenting investigative difficulties. Minimal training amongst judicial and forensic professionals coupled with evidential burden laid upon a claimant /prosecutor continue to facilitate the vice.

Apart from the germane issues of anonymity and evolution of cyber-crimes, jurisdictional challenges correspondingly heighten difficulties in the enforcement of laws against online crimes associated with fraudsters. Unlike other crimes where physical evidence easily secures convictions, online crimes profoundly rely on traces of internet activity which often provide little to no evidential value. In efforts towards addressing these criminalities, the Kenyan government in 2020 officially opened a forensic laboratory to tackle such sophisticated crimes. Despite this, little has been done in enhancing policing knowledge on evidence handling within the realm of cyber security.

Photo Credit: Guardian Nigeria

Unregulated financial technology

Kenya's National Computer Incident Response Team (KE-CIRT) financial report (2020), highlights cyber threats including digital fraud to have risen from 23 million in 2018 to 110 million in 2020. This suggests a positive relationship between rapid adoption of financial technology and increased threats posed by online fraudsters. In 2019, Kenya was ranked among the top three recipient countries of spam texts across the world, showing the magnitude of risks associated with the adoption of new tech-based advancements. In light of this 38.8 million cyber-attacks were recorded between April – June of 2021, showcasing an increase of 37.3% with about 27.4% of the incidents linked to online fraud. Thus, cyber-security advisories issued to companies around the same period tremendously increased by 3.693% in 2021 attributing to the growing number of cyber threat actors such as hacktivists, organized cybercriminals, and cyber terrorists. Hence, fast adoption of fin-tech innovations by consumers and investors despite lack of adequate information is a key cause of increased digital fraud in Kenya.

Photo Credit: Gigaspaces

Institutional security systems

Virtual attacks targeting vulnerable control systems within financial institutions have increased over the years pointing to the lack of effective security systems. Crimes such as identity theft, malware attacks and baiting have often been identified as leading causes behind digital fraud. Despite increased fraud risks within the sector, 21% of Savings and Credit Cooperative Organizations (SACCOs) do not carry out cybersecurity audits, while 48% only do so annually, as recommended.

Weak IT infrastructures continue to facilitate the susceptibility of financial establishments to attacks. In spite of this, most fiscal institutions dedicate funds to acquire/roll out technological infrastructure for growth, neglecting the need to incorporate or strengthen the infrastructure security systems. Additionally, compromised staff members within such institutions as well as government officials mandated with the collection of personal data have proved to be hindrances in the collective fight against online fraud. This has mainly been through lack of confidentiality and transparency. Breaches in consumer privacy amounting to lowered security standards has led to cases involving collusion between staff members of financial institutions and fraudsters. A case in point is the 2017 fraud incident where Kenyans lost KES 3.7 billion to foreign criminals in collaboration with local officials.

Photo Credit: outlook India

Conclusion

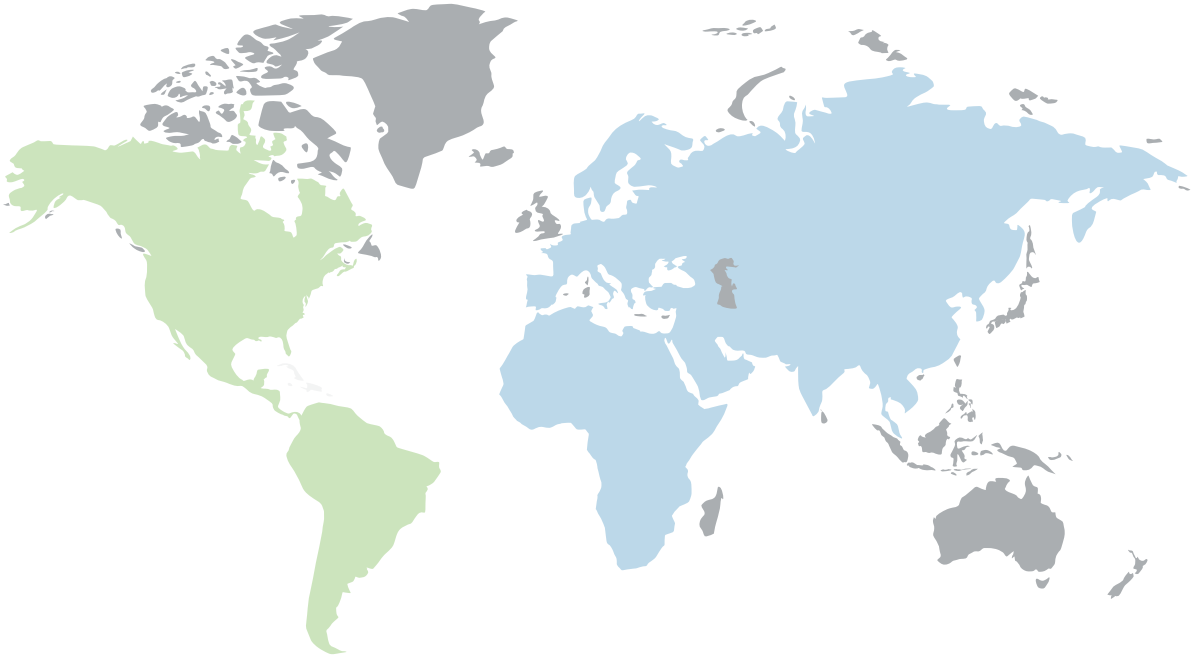
Kenya continues to experience losses to its economy due to digital fraud. The rise of unregulated fin-techs in addition to the lack of sufficient awareness amongst consumers in the financial sector continues to exacerbate the issue. Weak security control systems within financial institutions merged with inadequate legal and investigative expertise equally provide ripe grounds for digital fraudsters. Thus, policy interventions in tandem with the legislative buttressing of institutional regulations governing financial establishments should be prioritized.

Recommendations

1. The Ministry of Information Communications and the Digital Economy in collaboration with the Ministry of National Treasury and Planning should:
   a) promote public awareness campaigns on existing and emerging cyber-crimes targeting consumers and professionals in the financial sector.
   b) ensure finance-based institutions/establishments align and abide by the national stipulated security protocols to eradicate enablers of fraudulent activities.
   c) collaborate with the Ministry of Interior and Coordination of National Government and partner with stakeholders to curb the existence of fraudulent and unlicensed fin-tech firms.
   d) partner with the Judicial Service Commission to launch ICT stations in different county courts with an aim to enhance knowledge amongst judicial officials on digital crimes linked to financial services.
   e) collaborate with the Directorate of Criminal Investigations (DCI) with an aim to increase training activities amongst relevant law enforcement officials on the extraction, handling and investigation of digital fraud.
   f) partner with the Office of the Director of Public Prosecutions (ODPP) and Directorate of Criminal Investigations (DCI) in launching outreach training programs to enrich knowledge amongst law enforcement agencies on cybercrimes linked to online fraud.

Photo Credit: Source Holyrood

The GLOCEPS, Weekly Influential Brief *brings to policy makers precise incisive analyses of policy issues and events locally, regionally and globally. The priority is on topics that have a bearing on Kenya and beyond and are themed on defence and security; diplomacy and foreign policy; public policy, ethics and governance; strategic interests and transnational crimes; and development. We invite contributions from experts with policy opinions centred on any of the five pillars. Give us your thoughts and feedback through info@gloceps.org*



THE GLOBAL CENTRE FOR POLICY AND STRATEGY
(GLOCEPS)
Research | Knowledge | Influence

Off Kiambu Road, Nairobi Kenya
P.O. Box 27023-00100,Nairobi.
Telephone: 0112401331
Email: info@gloceps.org
Web: www.gloceps.org