MYRIAD Connect

Kenya Fraud Report:

Digital & Mobile financial transaction fraud 2018

As part of Myriad Connect's commitment to helping secure digital financial services and understand the unique requirements for Kenya, research was commissioned into the incidence of fraud in the market. Findings are detailed in this report.

The growth of Africa's lucrative banking and financial services market is largely attributable to the success of finacial technology, which has had a transformational impact across the continent, enabling financial inclusion and driving economic growth.

Disruptive payment tools like mobile money, mobile payment wallets and one click transactions are at the centre of this transformation in Africa and, backed by the strength of its success, Africa is poised to lead this transformation in the future.

While this technology continues to deliver innovative services to consumers, it has also presented fraudsters with opportunities to exploit weaknesses in systems to defraud customers. These fraudsters are finding ever more advanced ways of intercepting transactions or posing as customers to take their money, costing the industry dearly and eroding consumer confidence.

To understand the scale of the incidence of financial transaction fraud and the impact it has had on consumers, Myriad Connect commissioned research in the Kenyan market in 2018.

How does Kenya Transact?

Technology has played a transformative role in Financial Services, but these technologies have also exposed many vulnerabilities, which are helping to enable fraudsters.

So, while the introduction of mobile payments and other digital financial services have helped to drive financial inclusion and remarkable growth for the Kenyan economy, these digital channels are vulnerable to hackers who exploit them to compromise consumer accounts.

Outside of the use of cash, mobile money and traditional bank accounts are most popular with Kenyans.

57%

Mobile Money

40%

Bank Accounts

*Based on respondents to Kenya fraud survey

For those using bank accounts, mobile banking apps are the most popular means for transacting.

20%
Debit Cards

13%
Credit Cards

24%
Mobile Banking Apps

66%

Digital Payment Methods

Outside of using cash, there is a preference for digital payment methods in the Kenyan market

Financial transaction fraud in Kenya

- **57%** — Mobile Money
- **32%** — Mobile Banking
- **26%** — Online Shopping
- **21%** — Bank Cheque
- **20%** — ATM Card Skimming

*Based on whether respondents were victims or know victims of fraud per channel

Victims

71%

of Kenyans have been a victim of financial transaction fraud.

SIM swap

90%

of banking leaders identify SIM swap fraud as an issue plaguing the Kenya market.

What is SIM swap fraud?

One of the most prolific forms of financial transaction fraud in Kenya is SIM swap fraud.

- SIM swap is when a customer lets their operator know that their SIM card is damaged, lost or stolen
- The current SIM is deactivated and a new one issued
- Criminal groups work together to gather personal data and then pose as contract owners to secure a new SIM
- Once activated by the fraudster, they are able to access bank accounts and other sensitive data authenticated through the SIM

Losses per channel in Kenya

Losses of KES 5,001 - 15,000

- 21 % Online banking fraud
- 27 % Mobile money fraud
- 18 % Bank cheque fraud
- 21 % ATM card skimming
- 13 % Online shopping fraud

Losses of over KES 15,000

- 23 % Online banking fraud
- 27 % Mobile money fraud
- 23 % Bank cheque fraud
- 13 % ATM card skimming
- 14 % Online shopping fraud

46% **of fraud goes unreported**

64% **of victims don't get their money back**

How are victims compromised?

SMS	**57 %**
Phone call	**73 %**
Social Media	**17 %**
Email	**19 %**

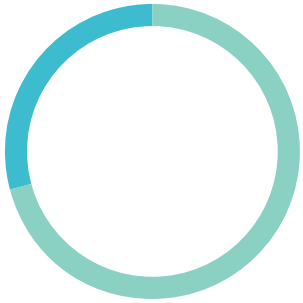
It is critical, therefore, that adequate security is provided for any digital transaction, helping to mitigate against risk for all stakeholders.

With the many challenges facing financial services, but also the limitless potential for growth and expansion in the industry, FinTechs have an instrumental role to play in propelling the industry forward. With a host of the world's most successful financial technology innovations borne in Kenya, many are looking to the country and its FinTech innovators to lead the way in driving financial services forward.

How are transactions secured today?

Use of on-time-password (OTP) via SMS for authentication of financial service transactions.

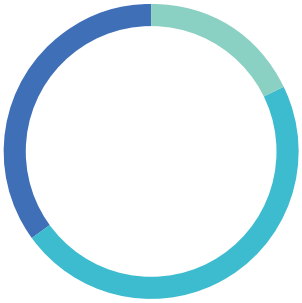
Use OTP via SMS for authentication of financial service transactions



71 %
Use OTP via SMS

29 %
Don’t use OTP via SMS

Frequency of OTP via SMS use for financial service transactions



18 %
less than once a month

47 %
min. once a month

35 %
min. once a week

The opportunity for financial service providers in Kenya

As technology advances in financial services, we are becoming more exposed to fraud and the impact on the industry both reputationally and financially is frightening.

However, there is an opportunity for financial service providers who are building brands around innovation and driving fintech, to be recognised as trusted providers to consumers. With the incidence of fraud rife in the market, many consumers feel like they are at risk of being defrauded via digital channels and are therefore looking for solutions and providers of secure financial services.

92 %

Move Bank

92% of Kenyans would move bank or financial service provider for an organisation that offers a more secure service to protect against fraud

83 %

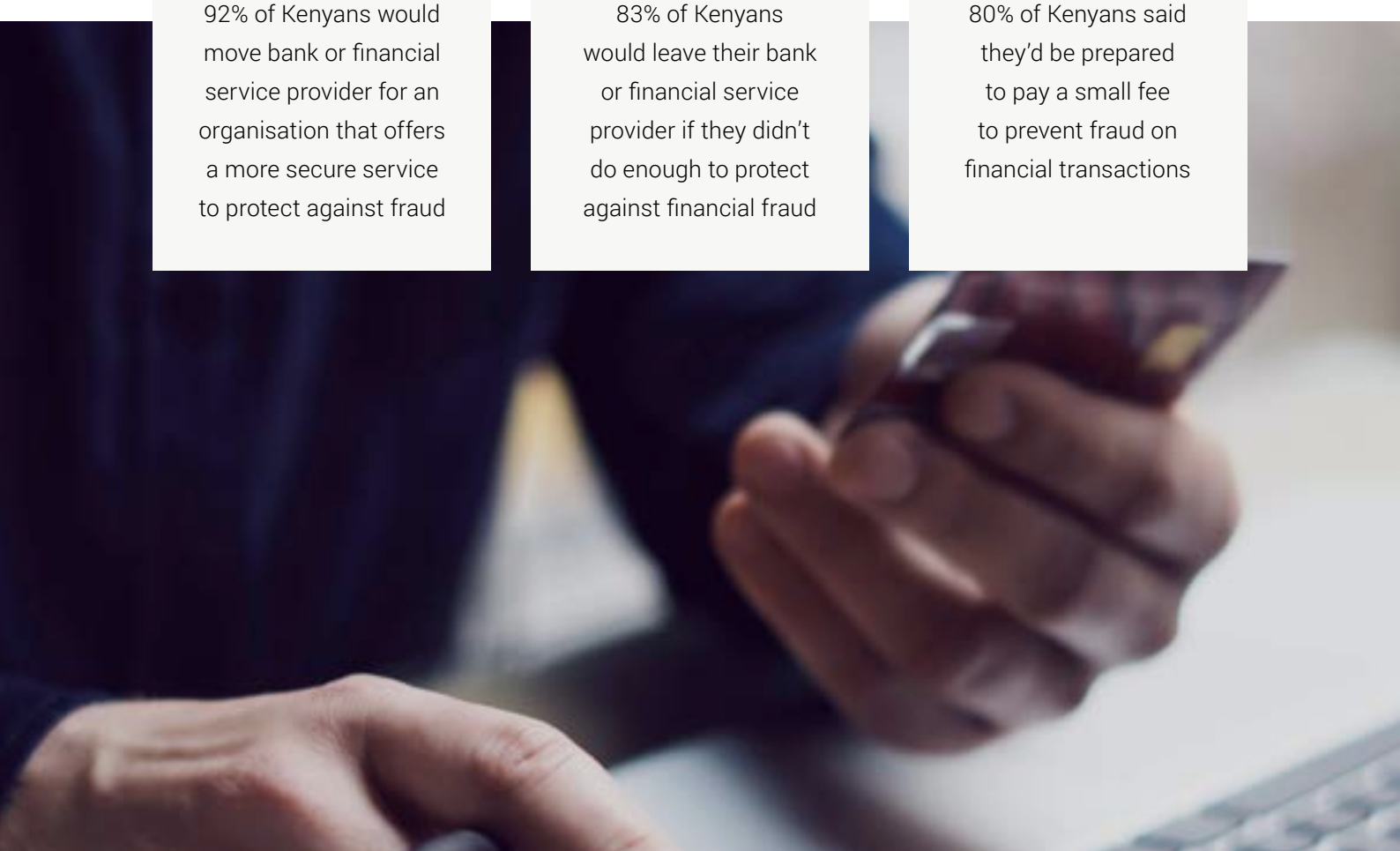
Leave Bank

83% of Kenyans would leave their bank or financial service provider if they didn't do enough to protect against financial fraud

80 %

Pay Fee

80% of Kenyans said they'd be prepared to pay a small fee to prevent fraud on financial transactions



Security should be at the heart of all digital financial services

As mobile and digital financial service adoption continues to grow, the range of new digital services will grow to deliver value to the expanding audience; which in turn will drive even further mobile adoption.

In the UK fraud prevention technologies have helped stop 67% of fraud attempts, so we can see this success in Kenya.

So, as financial service providers drive innovation in digital and mobile services, security needs to be at the heart of what you do.

67 %

Of fraud attempts stopped in UK using fraud prevention technologies.

£751

Value of prevented fraud

Financial fraud action UK report, Sept 2017

MYRIAD Connect

SIM swap detection & out of band authentication for financial services

Myriad Connect offers banks and financial service institutions out of band authentication and SIM swap detection services to empower them to protect each of their customers' financial services transactions.

Myriad Connect's market-leading authentication service delivers a separate, third party authentication channel on any mobile device.

Using Unstructured Supplementary Service Data (USSD) provides an entirely out of band channel for authentication, with all interactions transmitted over the mobile network, which is separate to the browser or online channel being used by the customer to initiate the transaction.

Myriad Connect's session-based service sends an advanced push notification to open up a conversation between the enterprise and customer. In addition, Myriad's SIM Swap detection service provides a real time check on the SIM, while no persistent data is held with any third party, providing a more secure service than current two factor authentication services. A clear audit trail is also established, where the user's identity is verified by a party external to the transaction. This results in a technology that greatly enhances the security of transactions vulnerable to SIM swap fraud. Myriad Connect partners with Financial service providers to ensure there is a heightened focus on security to help create superior digital financial services.

Service comparison

	SMS OTP	Mobile App	IMSI via MNO	Myriad advanced push
Content interception	EASY	DIFFICULT	DIFFICULT	DIFFICULT
Data not persistent	✗	✓	✓	✓
SIM swap secure	✗	N/A	✓	✓
Secure against 'man in the middle' attack	✗	✓	✓	✓
Mobile device compatibility	✓	✗	✓	✓
No data connectivity requirement	✓	✗	✓	✓
Country-wide network reach	✓	✗	N/A	✓
Entirely independent third party	✗	✗	✗	✓
Multi Channel (USSD, web, app, card, etc)	✓	✗	✗	✓

Our security promise

Myriad Connect's service requires no compromise on security, providing the universal reach of SMS, with a level of security beyond that delivered by mobile apps.

Myriad hereby provides organisations with an isolated, third party authentication channel on any mobile device providing world-class authorisation, access and authentication services.

Thank you.

https://connect.myriadgroup.com
info@myriadgroup.com

Securing Digital.