LEGAL TAKE

AN ONLINE DATA MINEFIELD

THE BANK'S ROLE IN SECURING SENSITIVE DATA SHARED ON THEIR DIGITAL BANKING PLATFORMS

Fidel Mwaki
Managing Partner

INTRODUCTION

Recently, I had a bit of trouble accessing my bank account through a digital banking platform. For whatever reason, the login credentials did not work, yet I was sure I had used the same ones recently and never shared them with anyone.

Cue slight panic, which led me to pay a visit to the local branch to see if they could figure it out for me. Needless to say, the bank official was efficient, helpful, and supportive, and my credentials were soon restored. While all ended well, the incident had me thinking about my personal data security in the digital era.

DIGITAL FINANCIAL PLATFORMS ARE A GOLD MINE OF SENSITIVE DATA

In recent years, many of us have become accustomed to using digital financial platforms to access our accounts and manage our funds. While this has improved our lives and the ease of doing business, often times we may not appreciate the huge amount of personal data that we share with our banks to help them identify us, store our information, and move our money locally and abroad.

A typical transaction through a digital banking platform involves sharing of certain personal data between banks and third parties. Right from the point you input a recipient's account information into the system up to the moment you submit the information for processing by the bank, the data flow tends to be swift and seamless – a testament to digital banking as an effective personal or business tool.

--- But that great impression has to be laced with some caution.

The information that a bank collects and processes has intrinsic value in the digital age. It is information that is personally identifiable and sensitive in nature and as a result should be processed by the bank within a secure framework to avoid being mishandled to the detriment of the customer.

Out of interest, I found time to peruse one bank's privacy policy statement, which showed that they collect the following information from consumers:

a) one's name, age, gender, sex, and identifying numbers,

b) one's physical and email addresses and contact numbers,

c) one's biometrics, race or ethnic origin, and personal and political beliefs,

d) one's online identifiers such as cookies and IP addresses, and

e) one's financial information.

This list is not exhaustive, and it is doubtful that many consumers will ever read it unless they happen to be very keen. Moreover, what may not be apparent to the consumer is whether any of the information collected by the bank is actually processed in line with the privacy policy statement.

WHAT ARE SOME OF THE BANK'S OBLIGATIONS UNDER THE LAW

Since the enactment of the **Data Protection Act, 2019** (the **Act**), Kenyan banks are now required to adjust to new legal standards affecting personal data and the rights of data subjects (in this case their customers). Given they are providers of financial services, banks are designated as data controllers and processors. As **data controllers** they determine why and how personal data should be processed and as **data processors** they actually process the personal data.

In digital banking, customer personal data is collected and processed electronically from the point it is supplied by the customer (as the end user) through inputs made on the digital financial platform. Consequently, banks operating digital banking platforms must comply with the Act in several ways:

1. Register with the Office of the Data Protection Commissioner (ODPC)

   Banks have a mandatory obligation to register with the ODPC as data controllers and data processors in accordance with the **Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021**.

   When registering, they must provide details of the categories of personal and sensitive personal data they collect and process and the purpose of processing (e.g., for KYC requirements or transactional purposes). They must also submit details on the category of recipients to whom persona data may be disclosed (e.g., regulators, other banks) and the technical measures they have put in place for protecting personal data collected on digital platforms.

2. Self-regulation and internal measures

In addition to registration, banks are required to self-regulate and ensure that adequate and sufficient safeguards and technical measures are put in place and fully adhered to. For example, digital platforms must be well maintained and secure with appropriate levels of security and reporting mechanisms, while banks should limit collection of personal information to that which is absolutely necessary to identify the parties to a transaction such as names, bank account numbers and the reason for the remittance.

3. Privacy policies and data protection agreements

Publishing of data privacy policies is critical to ensure that customers are made aware of the bank's guidelines towards handling customer personal data. This is particularly important when data is shared digitally as it tends to be easily collected, compartmentalized, and processed across several digital networks. The policies should be easily accessible to the customer and made available at the point of access or within the digital banking platform.

In addition, banks should have data protection agreements with third parties who process their customer's personal data locally and internationally. These parties may include local or international banks, mobile payment service providers and digital remittance operators. Robust agreements will guarantee that processing of personal data is protected across the chain of engagement.

4. Reporting requirements to regulators

Finally, given the importance of the banking sector to the general public, it is important for customers to appreciate that banks have legal obligations to report to regulators such as the Central Bank of Kenya and the Financial Reporting Centre who assign them a monitoring role in respect to transactions conducted within

their digital platforms. As a result, banks have to share personal data with such regulators when compelled to, and this is permissible under the Act.

CONCLUSION

Digital banking is a 21st century convenience that consumers should use with a sense of caution.

While banks must comply with legal requirements to ensure that customer information is processed within the law; it is incumbent upon consumers to stay informed and aware of their rights as data subjects to make sure they are not caught out by data breaches when transacting online.

On a personal note, I will certainly take a greater interest in my bank's policy statements on data security and third-party data use going forward.

In case you require further information on this topic or wish to learn more about data privacy, please contact **Fidel Mwaki** at legal@fmcadvocates.com

PUBLISHED BY

FMC ADVOCATES
2nd Floor, Left Wing
The Crescent, Off Parklands Road
Westlands
Nairobi - Kenya
www.fmcadvocates.com