DIGITAL BANKING AND PRIVACY IN ZIMBABWE: INVESTIGATING THE PRIVACY IMPLICATIONS OF DIGITAL BANKING SERVICES.

Research Report (2024) by Melissa Chasi

Table of Contents

INTRODUCTION

The Cyber and Data Protection Act[1] of Zimbabwe (CDPA) came into effect in 2021 and encourages the lawful use of technology by regulating the way data controllers process the personal data of Zimbabwean citizens. Under this Act, financial institutions fall into the category of data controllers since they determine the purpose and means of processing data. Mobile banking is defined in the Banking Act[2] as "an arrangement that allows a customer of a banking institution or licensee under the Postal and Telecommunications Act[3] to access any financial services through a mobile device". With banking technology evolving to the use of mobile applications and mobile money, privacy laws and regulations will have an impact on business operations, legal and financial penalties, customer requests as they exercise their new rights, a new regulator to report to and investments in technology to aid compliance.

Although the CDPA comes with additional expectations from the banks, Zimbabwean banks have already been seen to be the most readily compliant with data protection due to the stringent requirements of the Reserve Bank of Zimbabwe (RBZ) and their international partners. Some banks already follow the General Data Protection Regulations[4] (GDPR), so therefore data protection is not new to them. Even locally, rights to privacy and data protection provisions are found in The Constitution[5], the Consumer Protection Act, the Banking Act, and other guidelines provided by the RBZ.

[1] Cyber and Data Protection Act (Zimbabwe), 2021, Chapter 12:07
[2] Banking Act (Zimbabwe), 2000, Chapter 24:20
[3] Postal and Telecommunications Act (Zimbabwe), 2000, Chapter 12:05
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
[5] Constitution of Zimbabwe, 2013

Though privacy is not completely new to banks, the culture of privacy still needs to be fostered for employees and the rest of society as a whole still does not understand the importance of privacy and this gap needs to be closed. With the increase in data breaches around the world and some reported in Zimbabwe, the CDPA gives banks guidance on their obligations as data controllers to data subjects and the Data Protection Authority.

This paper therefore seeks to explore how the Act will shape the way banks and mobile money providers will handle, process, and protect personal data in the provision of their digital services.

RATIONAL & RESEARCH GOAL

Although banks in Zimbabwe are already subject to stringent RBZ requirements, the introduction of the CDPA and its associated regulations imposes an additional layer of obligations. This research aims to explore the evolving privacy landscape in Zimbabwe's banking sector, analysing how the Act impacts business operations, institutional culture, and the consequences of non-compliance.

The specific objectives of this study are:

- To examine the current privacy approaches of financial institutions in Zimbabwe since the introduction of the CDPA.
- To assess the necessary steps for ensuring compliance with the CDPA and what these requirements will mean for banks.
- To offer policy recommendations for financial institutions and other key stakeholders, focusing on bridging the gap between policy, technology, and societal needs.

RESEARCH METHODOLOGY

This research, conducted over two months (August–September 2024), is ongoing. The study involves analysing key legislation relevant to digital banking and privacy in Zimbabwe, such as the Cyber and Data Protection Act and regulations, the Banking Act, RBZ cybersecurity guidelines, consumer protection frameworks. Additionally, privacy policies from interviewed financial institutions were examined.

A qualitative approach was employed, with interviews conducted among six institutions: three banks and three fintech companies. The interviews covered themes such as compliance practices, data privacy governance, customer communication strategies, and contributions to policy development. Out of the six participants, one responded via a Google form survey, limiting the depth of their response. However, five participants engaged in either in-person or virtual interviews, with the majority being from compliance departments. A limitation of relying on the compliance team was that when it came to technical questions for example what tools are employed to delete a customer's data, they said the IT department would be more knowledgeable about that. One participant represented the technology team, but this presented another limitation, as they were unable to address customer communications issues and other compliance issues. Overall, the compliance team was well placed to deal with the interviews as they are currently dealing with data protection issues across the sector.

Consent and anonymity were assured due to the sensitivity of the information. Additionally, an interview with the Data Protection Authority provided insights into the current state of privacy regulation in Zimbabwe. The themes discussed included regulatory enforcement, institutional support, challenges faced, and public awareness of data subject rights. The Authority was forthcoming and shared data controllers' and data subjects' reports. There was also a case study of Barclays Bank UK which served as an example of a user journey that prioritises data protection.

FINDINGS AND DISCUSSIONS

Current Privacy Practices in Banking Sector

Financial institutions worldwide operate under stringent regulatory frameworks, both locally and internationally. In Zimbabwe, the primary regulatory authority is the Reserve Bank of Zimbabwe[6]. When queried about their adherence with data protection frameworks, all institutions interviewed cited adherence to the European Union's General Data Protection Regulation (GDPR), ISO/IEC 27001[7], and one referenced South Africa's Protection of Personal Information Act[8]. This reliance on international best practice is driven by the requirements of their global financial partners, this indicates the sector's pre-existing awareness of data privacy prior to the enactment of the CDPA in 2021.

However, implementing the CDPA has proven challenging due to the absence of complementary regulations, which were only gazetted on 13 September 2024[9]. These regulations[10] provide critical clarifications concerning deadlines, penalties, the licensing of data controllers, and the appointment of Data Protection Officers (DPOs). The delay in publishing these regulations created a guidance vacuum, suggesting that data protection was not a priority for the Data Protection Authority (DPA).

The DPA, in conjunction with the Minister of Information and Communication Technology, had drafted regulations for submission to the Attorney General's Office in 2022. This indicates that the proposed regulations were under review for two years. The excuse the DPA was given was that there was a shortage of skilled human resources, this was exacerbated by a significant brain drain as professionals migrated abroad in search of better opportunities. This delay illustrates how broader economic challenges are affecting Zimbabwe's ability to implement robust data privacy frameworks. Without a skilled workforce, it is difficult for regulators to keep pace with the evolving demands of data protection, potentially compromising the rights of data subjects and creating inconsistencies in compliance.

The impact of this delay is evident in the banking sector, where regulatory uncertainty has led institutions to adopt privacy practices shaped by international best practices. While this allows for a degree of protection, it also creates a risk that local laws, such as the CDPA, may be overlooked. Privacy officers within these institutions must ensure compliance with evolving local regulations, even as they strive to meet global standards.

All six financial institutions interviewed had privacy policies available on their websites and they largely adhered to data protection principles as shown in the table below.

COMPARATIVE PRIVACY POLICY ANALYSIS

	Consent	Purpose Limitation	Data Minimisation	Data Subject Rights	Data Security Measures	Data Retention	Data Sharing	CDPA Mentioned
Bank 1	yes	yes	yes	yes	yes	yes	yes	yes
Bank 2	yes	yes	yes	yes	yes	yes	yes	no
Bank 3	yes	yes	yes	yes	yes	yes	yes	yes

[6] https://www.rbz.co.zw/

[7] ISO/IEC 27001:2013 – Information Security Management Systems – Requirements.

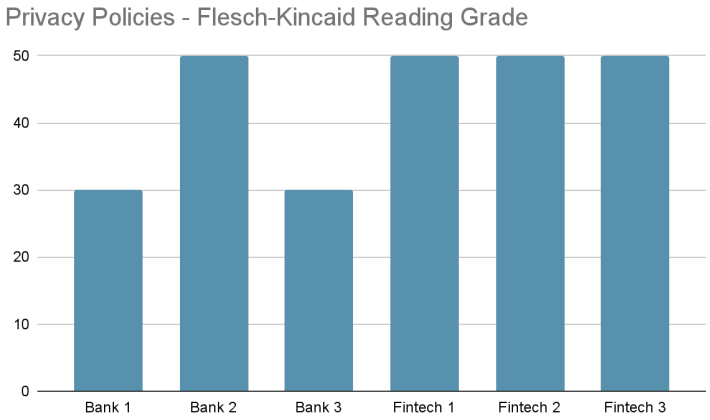
[8] **Protection of Personal Information Act (POPIA)** (South Africa), 2013, Act No. 4 of 2013.

[9] **Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations**, 2024, **Statutory Instrument 155 of 2024**.

Fintech 1	yes	yes	yes	yes	yes	yes	yes	no
Fintech 2	yes	yes	yes	yes	yes	yes	yes	no
Fintech 3	yes	yes	yes	yes	yes	yes	yes	no

However, it was concerning to note that only two of the six institutions specifically referenced the CDPA in their policies. Mentioning the legislation they are compliant with is crucial as it helps users understand the legal framework governing their personal data. The absence of such references in the majority of policies suggests that there is still a lack of full integration of the CDPA into their operational frameworks.

Wagner (2021) found that privacy policies are often excessively lengthy and challenging to comprehend, resulting in most users neglecting to read them. This trend indicates that organizations primarily craft privacy policies to satisfy regulatory requirements rather than to genuinely inform data subjects about their data privacy practices. To evaluate the readability of the privacy policies from the interviewed institutions, the Flesch-Kincaid Readability Test[11] was used via an online calculator that uses their formula[12]. The findings revealed that two banks scored within the 0-30 range, categorising their documents as very difficult to read and accessible only to university graduates. The remaining institutions scored between 30-50, indicating a level of difficulty that is limited to university educated individuals.



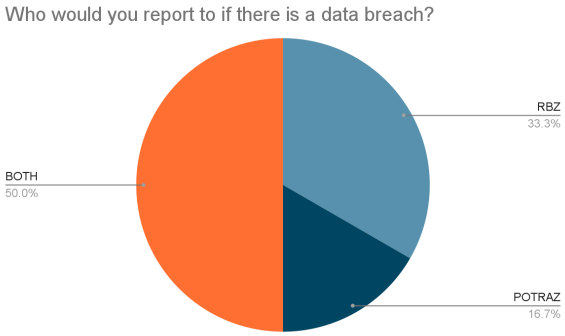
In the context of Zimbabwe's financial institutions, comprehension of these policies is further complicated by language barriers, as all policies are presented in English, while the predominant national languages are Shona and Ndebele. This raises the need for innovative solutions that are centred on customer comprehension of data privacy practices. For instance, Barclays Bank UK has a video clip of less than two minutes that effectively communicates essential information about personal data[13]. Additionally, their privacy notice pages feature accessible panels with bite-sized information, enabling customers to better understand and retain control over their personal information. Zimbabwean banks could benefit from adopting similar approaches.

[11] Flesch, R. & Kincaid, J.P., 1975. *General readability formula*. *Reading Research Quarterly*, 10, pp.22-23.
[12] https://serpninja.io/tools/flesch-kincaid-calculator/
[13] https://www.barclays.co.uk/important-information/control-your-data/

Compliance with the CDPA

Reporting to a New Authority

All banks must be licensed to operate as data controllers, as they "determine the purposes and means of processing personal data"[14]. While financial institutions have traditionally reported to the RBZ, they now have to report to the DPA. An interview with the DPA revealed that they have a Memorandum of Understanding with the RBZ, facilitating quarterly meetings to collaborate and address grey areas. For instance, when mobile money services emerged, it was unclear who held responsibility, given that these services operate as quasi-banks under the RBZ while also being linked to telecommunications companies licensed by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). Ultimately, these issues were determined to fall under the purview of the RBZ.



When asked about reporting procedures in the event of a data breach, the responses from the interviewed institutions varied, indicating some confusion regarding the appropriate authority. To ensure uniformity across the sector, both authorities must provide clear, consistent guidance. Financial institutions should prepare for further gray areas with the new Act, as there may be tensions between established banking practices and emerging data protection principles.

So far, the Data Protection Authority (DPA) has registered 115 data controllers, including 75% of financial institutions, signaling a promising willingness to cooperate. Some banks have even requested certificates of compliance to present to their international partners, an initiative the authority plans to implement following these requests.

Before the regulations were published, several banks sought advice on training employees in data protection, guidance on automated processing for credit bureaus, and approaches to data privacy during mergers and acquisitions, as well as timelines for compliance. Section 6 of the CDPA allows the DPA to issue opinions or advice to anyone with a legitimate interest, and they have actively engaged with those who reached out. This reflects a more collaborative approach to compliance with the regulator, as opposed to a punitive one. The regulations provided clarity regarding compliance timelines: data controllers have three months to appoint a compliant Data Protection Officer (DPO) and six months to submit an application for a data controller's license.

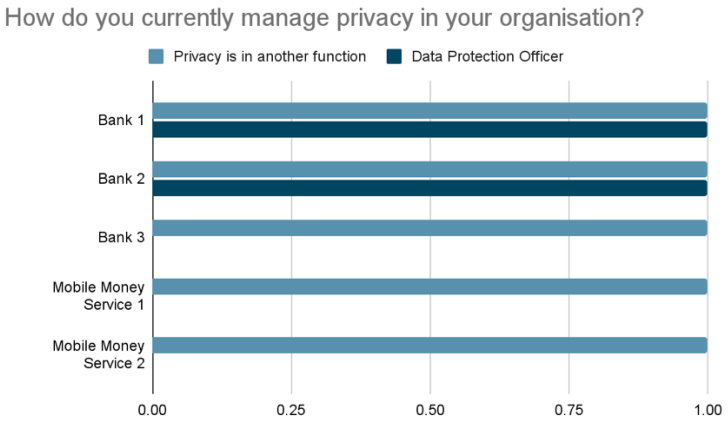
The Authority also possesses the power to conduct ad hoc inspections, investigate complaints from data subjects, issue non-compliance notifications, and seek court orders to halt the processing of personal information. Such actions could be detrimental to a financial institution, motivating them to prioritize compliance. However, it is essential to note that while the DPA holds these powers, it faces resource constraints with a team of less than 20 people. Given the vast number of data

[14] **Cyber and Data Protection Act** (Zimbabwe), 2021, Chapter 12:07, s.3

controllers across various sectors, it will be challenging for this small team to carry out physical inspections effectively. Established in 2023, the DPA is still in its infancy, but with time, it is expected to grow and enhance its capacity to enforce the CDPA.

Appointing DPOs

In interviews with financial institutions, only 2 out of 5 reported having a certified Data Protection Officer (DPO). According to the regulations, a DPO must be certified by the Data Protection Authority in collaboration with a recognized higher learning institution, meaning that foreign privacy certifications are not accepted for practicing as a DPO in Zimbabwe. Responses from the institutions indicated that none had a dedicated privacy function; instead, privacy-related matters were handled within other departments, primarily the compliance department. Institutions without certified DPOs expressed intentions to certify their personnel to ensure compliance. Section 12(6) of the regulations specifies that failure to appoint a DPO may result in a fine not exceeding level 7 and/or imprisonment for up to two years. This underscores the necessity of appointing a DPO as a critical first step toward compliance CDPA.



Legal Implications

S. 33(2) of the CDPA imposes substantial penalties on data controllers, their representatives, agents, or assignees for breaches of their responsibilities as outlined in S. 11, 13, 18(4), 24, and 28. Violators face fines of up to level 11 and/or imprisonment for a maximum of seven years. Statutory Instrument 14A of 2023 establishes that level 11 fines amount to approximately US$1,000. This figure is disappointing and does not reflect the seriousness that data protection necessitates; for banks and large organizations, this fine is relatively inconsequential and unlikely to serve as an effective deterrent.

Moreover, the CDPA currently does not grant the Data Protection Authority (DPA) the authority to impose fines, rendering it ineffective in enforcing compliance. In contrast, the General Data Protection Regulation (GDPR) empowers authorities to impose significant fines—up to €20 million or 4% of the total global turnover from the previous financial year, as stipulated in Article 58(2)(i)[15]. The GDPR mandates that fines be "effective, proportionate, and dissuasive," a standard not met by the current fines in Zimbabwe.

[15] European Parliament and Council of the European Union. (2016). Article 58 of Regulation (EU) 2016/679. In *General Data Protection Regulation*.

While the provision for imprisonment could hold employees or agents of data controllers personally liable, thereby encouraging a more serious approach to data privacy, it raises questions about accountability within organizations. Specifically, it remains unclear who within an organisation would bear responsibility for data protection violations.

Comparing Data Protection Principles vs Banking Sector Requirements

Data Minimisation and Know Your Customer (KYC)

Privacy regulations necessitate that financial institutions strike a balance between data protection principles and existing sector-specific requirements[16]. One of the core principles of data protection is data minimization, which mandates that data controllers collect only information that is necessary for their primary purpose of processing. This principle aims to prevent the excessive collection of customer information.

However, financial institutions in Zimbabwe are also bound by the Bank Use Promotion and Suppression of Money Laundering Act**,** which promotes the use of the banking system while suppressing its abuse. Section 24 of this Act requires institutions to "verify customers' identity" using an identity document[17]. While this requirement is not prescriptive, it mandates banks to take "reasonable steps" to confirm the true identity of their customers. This flexibility implies that banks may require more information than merely an identification document to ensure they understand their customers thoroughly.

In practice, the banks interviewed reported requesting a range of documentation beyond just a National ID. These included passport photos, proof of residence, and an initial deposit. The account opening forms provided further opportunities for banks to collect additional customer information, some of which raised concerns regarding relevance. Notably, some banks requested social media details from platforms like Facebook, Skype, Twitter, and LinkedIn, as well as information about customer hobbies. The relevance of this information is often not explained, and the collection of social media data could potentially lead to monitoring or misuse by banking employees.

The RBZ adheres to the Financial Action Task Force (FATF) requirements, which encourage banks to implement a risk-based approach (RBA) to customer due diligence[18]. Under this approach, higher-risk customers, such as foreigners and politically exposed persons (PEPs), are subject to more extensive information collection and monitoring, whereas lower-risk customers face simplified due diligence requirements. This practice aligns with the principle of data minimisation, as only the necessary information is gathered based on the risk profile of each customer. For higher-risk groups, banks might collect additional information to ensure adequate scrutiny, in line with the *RBZ's Anti-Money Laundering (AML) Risk-Based Oversight and Supervision Guidelines*.[19]

Similarly, s. 7(1)(a) CDPA supports the concept of data minimisation by stipulating that data controllers should collect only data that is relevant and necessary for the specified purpose. Thus, by adopting the RBA and adhering to KYC requirements, Zimbabwean banks ensure that they comply with both data protection and financial sector regulations while maintaining an efficient balance between the two.

Data Breach Notification and Safe Custody

[16] Greenleaf, G. and Tyree, A. (2017). Bankers' Duties and Data Privacy Principles: Global Trends and Asia Pacific Comparisons In: *Can banks still keep a secret?* Cambridge University Press, pp. 31-61.
[17] *Bank Use Promotion and Suppression of Money Laundering Act [Chapter 24:24]*. Government of Zimbabwe.
[18] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf
[19] https://www.rbz.co.zw/documents/nps/AML-RBA-OVERSIGHT-GUIDELINE-2021.pdf

S.18(1) of CDPA mandates that data controllers "take the appropriate technological and organizational measures necessary to protect data from negligent or unauthorized destruction, negligent loss, unauthorized alteration or access, or any other unauthorized processing of data." Banks are already obligated to maintain secrecy[20] over customer information and are entrusted with the safe custody of this data. To meet these responsibilities, banks will need to invest in advanced technologies to ensure that personal data is adequately protected, as breaches carry severe consequences. Therefore, s.18 primarily reinforces existing duties of confidentiality for banks.

However, new obligations arise concerning data breach notifications. Under Section 19 of the CDPA, banks must notify the Data Protection Authority (DPA) in the event of a data breach. Furthermore, prior to the regulations, Zimbabwean banks were not legally obligated to inform customers of data breaches. Under the new law, they must notify customers within 72 hours if a breach occurs.

However, banks are only required to notify customers if the breach presents a high risk of infringing on their rights and freedoms. This necessitates a risk assessment to determine whether a data breach merits disclosure to affected individuals. This creates a potential gap, as banks might be inclined to classify breaches as low-risk to avoid reputational damage and the loss of customer trust. In the writer's opinion, data subjects should be informed of any breaches involving their personal information, regardless of the risk assessment outcome.

Among the institutions interviewed, none reported having experienced a data breach. This is unsurprising, given the industry's culture of secrecy. Admitting to a data breach could severely damage a bank's reputation and potentially lead to customer loss, making transparency difficult.

Data Retention and Destruction

s.25 (2) of the Banking Act states that customer records must be kept for at least 5years from date of transaction completed[21]. This requirement is crucial for ensuring that financial transactions remain traceable in case of future investigations. However, this regulatory obligation poses a potential conflict with the data retention principle under data protection laws, which stipulates that personal data should not be kept longer than necessary for the purposes for which it was collected. Unlike the Banking Act, the data retention principle does not specify a maximum retention period.

This lack of specificity means that financial institutions must determine appropriate retention limits and justify their decisions based on the purposes for which the data was initially collected. The absence of a clear-cut maximum retention period may lead to inconsistencies in data retention policies across different banks. Therefore, it may fall upon the relevant regulators—such as the Reserve Bank of Zimbabwe (RBZ) and the Data Protection Authority (DPA)—to collaborate with financial institutions and stakeholders to establish an upper limit on data retention, ensuring uniformity and compliance with both legal and data protection requirements.

Customers as Data Subjects

S. 48 and 49 of the Consumer Protection Act (CPA) grant customers the right to privacy, confidentiality, and the ability to restrict unwanted direct marketing[22]. The RBZ's Consumer Protection Framework (CPF) reinforces these protections, requiring banks to safeguard customer data, use it for specified purposes, and obtain prior consent[23]. Customers also have the right to file complaints, and banks must maintain clear channels for these. Additionally, banks are required to update customer information, such as changes in address or name (e.g., due to marriage). These protections align with the rights of

[20] Banking Act Chapter 24:20; s.76
[21] Banking Act Chapter 24:20; s.25(2)
[22] *Consumer Protection Act [Chapter 14:44].* Harare: Government of Zimbabwe.
[23] https://www.rbz.co.zw/documents/consumer_protection/consumer-protection-framework-26-june-2017.pdf

data subjects under the Cyber and Data Protection Act (CDPA), including the right to be informed, give and withdraw consent, rectify data, and complain—well-established in prior legislation.

The CDPA introduces new rights that will affect financial institutions' operations, particularly the right to access information (s.14(b)), the right to erasure, and the right to withdraw consent. These rights require new processes and technologies to ensure their effective implementation. For instance, only one bank surveyed had an automated system to handle data erasure requests, while others were uncertain. Although banks are legally required to retain data for at least five years, systems must be in place to process deletion requests once the retention period has expired.

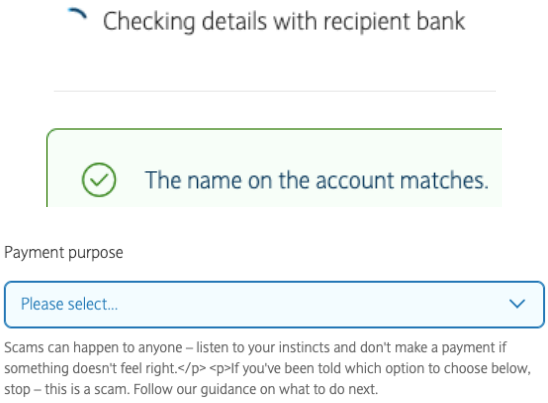
Similarly, exercising the right to access data will require banks to address issues such as authentication, data storage, response time, and secure transmission. Ensuring security at each stage is crucial, as these processes could expose banks to new vulnerabilities.

These new rights promote greater transparency and accountability, requiring banks to respond diligently to data subject requests while maintaining security. In the event of a data breach, banks must notify affected customers within 72 hours. Ultimately, financial institutions will need to invest in both technology and human resources to ensure customer data is properly protected.

A Case Study: Barclays Bank UK User Journey

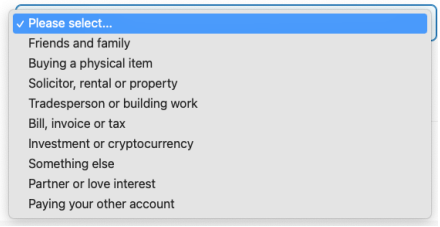
The customer journey on the Barclays online banking application offers valuable insights into how privacy and security are handled, which Zimbabwean banks could learn from.

Step 1: Transaction Verification When initiating a payment, Barclays checks the recipient's account details with the other bank to confirm accuracy before processing the transaction. This system helps prevent errors. In contrast, local Zimbabwean banks often allow transactions with incorrect recipient details, creating inconvenience and delays in reversing payments.

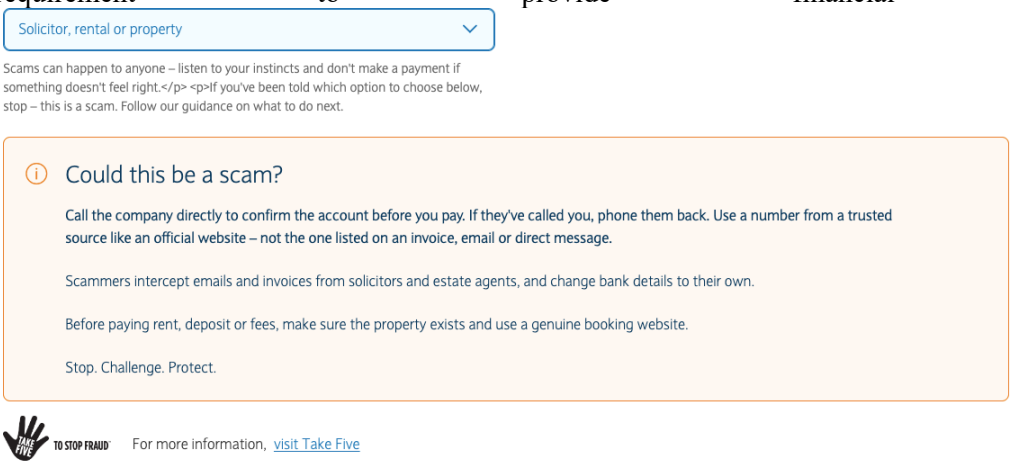


Step 2: Scam Awareness Barclays provides a warning about potential scams during the transaction process, prompting customers to think critically before proceeding. In Zimbabwe, mobile banking apps do not offer similar warnings. Instead, banks often disclaim responsibility for losses due to network or third-party issues, placing the burden on customers[24]. Educating customers at this stage on scams and security risks would align with the RBZ's consumer protection framework, which mandates financial education.

[24] An example - "Note: I/We hereby indemnify xxx, its officers, agents and employees against any losses of claims resulting from events or occurrences beyond its control including but not limited to challenges arising from telecommunications infrastructure, connectivity and services of the various network operations. The onus is upon me/us to confirm with the beneficiary that the funds have been received."

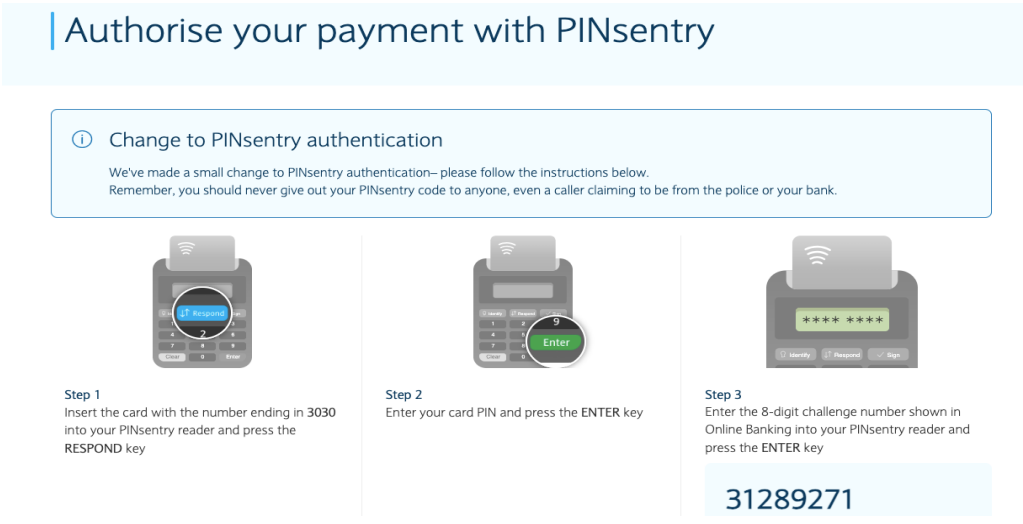


Step 3: Payment Purpose Confirmation Before completing a transaction, Barclays requires customers to confirm their understanding of potential risks, including scams. This proactive approach encourages due diligence. Zimbabwean banks could adopt a similar feature, particularly for transactions related to black-market currency exchanges, which are prone to scams. Such measures would fulfill the RBZ's requirement to provide financial education.



Step 4: Customer Verification Barclays uses a PINsentry card reader and mobile PINsentry for added security, ensuring that only the authorised customer can complete transactions. This multi-layered verification process is a model for local banks, highlighting the need for investments in security technology and expertise to protect customer data effectively.

By integrating customer education during transactions and implementing advanced verification systems, Zimbabwean banks could enhance security and compliance while promoting financial awareness.



RECOMMENDATIONS

Recommendations for Financial institutions

1. Financial institutions should analyse how banks in other jurisdictions, like Barclays, manage data privacy to identify effective strategies and apply them locally.
2. Engage the marketing team to develop creative ways of presenting privacy policies, such as through videos, making them more accessible and engaging for customers.
3. Establish a standalone privacy function instead of overburdening compliance teams. This ensures focused attention on privacy compliance, improving the overall quality of data protection.
4. Ensure privacy policies are not just theoretical but practical. Mechanisms must be in place for data subjects to exercise their rights, such as the right to deletion, which goes beyond simple email requests.
5. Regular DPIAs will help institutions identify gaps and assess their current standing on data protection and privacy.
6. Incorporate customer financial education during their user journey on your mobile application in addition to awareness campaigns to educate customers about their data privacy rights and how banks protect their personal information.

Recommendations for Regulators

1. Introduce clear compensation mechanisms for customers affected by data breaches to enhance accountability.
2. Impose higher fines for non-compliance to reinforce the seriousness of data protection laws.
3. Launch broader public awareness campaigns to educate the market on data privacy, making the issue more visible. There is need to invest in marketing campaigns across sectors.
4. The Data Protection Authority should engage more frequently and transparently with financial institutions and the public to ensure clear expectations.
5. Encourage institutions to establish privacy as a standalone function, similar to compliance or risk, for stronger oversight.
6. Avoid duplicative reporting by establishing clearer collaboration between the Reserve Bank of Zimbabwe and the Data Protection Authority, ensuring streamlined processes.