The speed of money: Ensuring data privacy in South Africa's instant payment systems

Nolwazi Hlophe | Senior Fintech Specialist at the Financial Sector Conduct Authority (FSCA)

In today's fast-paced world, instant payments make a huge difference. We are able to move money within minutes – or even seconds – anytime of day or night, 24/7. But while the speed and efficiency of the latest digital payment systems in South Africa offer fantastic benefits, they also bring unique challenges that necessitate a closer look. A particular concern is the privacy and security of our personal data.

The rise of instant digital payments and data's new role

Fast digital payment systems are designed to process transactions in real-time, offering immediate availability of funds and certainty that a payment has gone through (SurePay, n.d.). This speed relies heavily on the seamless flow of data.

While convenience is undeniable, the stakes for data privacy are higher than ever.

Every time you make an instant digital payment, a wealth of personal information is involved: your account details, transaction history, and often, details about what you're buying or who you're paying. This data is incredibly sensitive, and its widespread collection and use create new privacy risks, including potential misuse for targeted advertising or even price discrimination (Bank for International Settlements [BIS], 2025).

The sheer volume and speed of these transactions also make them attractive targets for cybercriminals looking to exploit vulnerabilities. Fraud, money laundering, and other illicit activities can leverage the instant nature of these systems to move funds quickly and undetected (World Bank, n.d.).

Navigating the regulatory landscape: POPIA

To counter these risks, robust data privacy legislation is essential. South Africa's **Protection of Personal Information Act, 2013 (Act No.4 of 2013) (POPIA)**, fully enforced since July 2021, is our cornerstone in this regard. POPIA seeks to protect natural and juristic persons from harm by protecting their personal information.

POPIA is built on principles like accountability, transparency, security, data minimisation, and, crucially, the rights of individuals regarding their personal information (Standard Bank, n.d.). This means organisations handling your data must be transparent about what they collect, why they collect it, how long they keep it, and how they protect it. Organisations also need your consent to process your personal information, including things like direct marketing (PayFast, n.d.; Baker McKenzie, 2025). Non-compliance with POPIA can lead to significant consequences, including substantial fines, up to R10 million for serious offences (PayFast, n.d.).

Let's look at some specific sections of POPIA that are particularly relevant to digital payment processing and safeguarding your financial data:

- **Chapter 3: Conditions for Lawful Processing[1].** This section deals with foundational principles and conditions that govern the lawful processing. It states that personal information, including your payment details, may only be processed if certain conditions are met. These include:
    - **Consent (Section 11(1)(a)):** Your voluntary, specific, and informed consent for the processing of your personal information. While POPIA isn't *always* consent-driven and outlines several other justifications for processing personal information, for many payment-related activities, especially those beyond the direct necessity of a transaction, consent is crucial (Michalsons, n.d.). This means that under POPIA, organisations must get explicit consent for payment-related activities that go beyond what is directly necessary to complete a transaction, as other legal justifications for processing personal information don't apply.
    - **Necessity for Contract (Section 11(1)(b)):** Processing is necessary to carry out actions for the conclusion or performance of a contract to which you are a party. This covers the direct processing needed to complete a payment transaction. This means an organisation can use your personal information, such as your payment details, to complete a purchase you've made because it is essential for fulfilling the agreement between you and the organisation.
    - **Compliance with Legal Obligation (Section 11(1)(c)):** Processing is required to fulfill an obligation imposed by law. This means an organization can process your personal information, like your identity documents, because a specific law—such as the Financial Intelligence Centre Act (FICA) for banks—requires them to do so.

[1] Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use.
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

    - **Legitimate Interest (Section 11(1)(f)):** Processing is necessary for pursuing the legitimate interests of the responsible party[2] or a third party to whom the information is supplied. However, this must be balanced against your rights and interests. This means an organization can process your personal information if it's necessary for their own reasonable business activities or for a third party they're working with, as long as it doesn't unfairly infringe on your rights and privacy as the individual whose information is being used.
- **Section 19: Security Safeguards.** This section is critical for protecting payment data. It requires responsible parties to secure the integrity and confidentiality of personal information in their possession or under their control. This involves implementing "appropriate, reasonable technical and organisational measures" to prevent loss, damage, unauthorised destruction, and unlawful access or disclosure of personal information. For payment systems, this translates to robust cybersecurity, encryption, and access controls (POPIA, n.d. - Section 19).
- **Section 20: Information Processed by an Operator.** Many payment service providers act as "operators" on behalf of banks or merchants ("responsible parties"). This section mandates that an operator must process personal information only with the knowledge or authorisation of the responsible party and must treat such information as confidential (POPIA, n.d. - Section 20; SimplePay, n.d.).
- **Sections 105 and 106: Unlawful Acts in Connection with Account Numbers.** These sections specifically address the misuse of account numbers, which is defined as unique identifiers that have been assigned to you, which are central to payment transactions.
    - **Section 105** outlines offences for a "responsible party" (e.g., a bank or a payment service provider directly handling your data) if they unlawfully process your account number, especially if it's of a severe or persistent nature and causes substantial damage or distress (POPIA, n.d. - Section 105).
    - **Section 106** extends this to "third parties" who knowingly or recklessly obtain, disclose, or procure the disclosure of an account number without the consent of the responsible party. It also makes it an offence to sell or offer to sell account numbers obtained in contravention of the Act (POPIA, n.d. - Section 106). These sections highlight the severe legal consequences for mishandling sensitive financial identifiers.
- **Section 22: Notification of Security Compromises.** Suppose there's a security breach involving personal information, including payment data. In that case, the responsible party must notify the Information Regulator and the affected data subjects (you!) as soon as reasonably possible (POPIA, n.d. - Section 22). This ensures transparency and allows you to take protective measures.
- **Sections 23, 24, 25: Data Subject Participation.** These sections empower you with rights over your data. You have the right to request access to your personal information, to ask whether information about you is being held, for corrections if it's inaccurate, or excessive, and to request its destruction or deletion in certain circumstances (POPIA, n.d. - Sections 23-25).

[2] Responsible party means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

POPIA empowers you with rights, such as the right to access your data, request corrections, and, in certain circumstances, have your data deleted. These rights are vital in maintaining control over your digital footprint in the age of instant digital payments.

Comparing with the European Union's strict standards

The General Data Protection Regulation (GDPR) in the European Union sets a strong precedent that many other countries, including South Africa with POPIA, have drawn inspiration from. GDPR applies to any meaningful information related to an identifiable person and classifies payment data as highly sensitive (GDPR.eu, n.d.). It mandates strict data protection standards for payment processing, requiring "Privacy by Design" (building privacy into systems from the outset) and "Data Minimisation" (collecting only necessary data) (Juspay, n.d.).

Businesses must also be transparent about data handling through clear privacy notices and ensure strong security measures like encryption (GDPR.eu, n.d.). Non-compliance with GDPR can result in hefty fines, up to €20 million or 4% of a company's global annual turnover (GDPR.eu, n.d.).

Securing our data in the fast lane

So, how do digital payment systems balance speed with robust data privacy? It's a complex task, but several key security measures are being widely adopted:

- **Encryption:** This involves transforming sensitive data into unreadable codes during both transmission and storage, making it unintelligible to unauthorised parties. Protocols like TLS (Transport Layer Security) are essential for securing data as it moves across networks (Stripe, n.d.).
- **Tokenisation:** This is a highly effective method where sensitive payment information, like your credit card number, is replaced with a unique, meaningless "token" (Stripe, n.d.; Square, n.d.). The actual sensitive data is stored securely in a separate, highly protected "vault", and only the token is used for transactions. If a token is compromised, it has no intrinsic value and cannot be used to conduct fraud (Worldpay, n.d.). This significantly reduces the risk of data breaches and helps businesses meet compliance standards like the Payment Card Industry Data Security Standard (PCI DSS) (Square, n.d.; G2 Learning Hub, 2025).
- **Multi-Factor Authentication (MFA):** Adding extra layers of verification, beyond just a password, significantly enhances security. This could involve a combination of something you know (like a password), something you have (like your phone for an OTP), or something you are (like a fingerprint) (Chargeflow, n.d.; Stripe, n.d.).
- **Robust Fraud Detection Systems:** With real-time payments, the ability to quickly identify and prevent fraudulent transactions is paramount. Systems use machine learning and behavioural analysis to detect suspicious patterns and block fraudulent activity before it completes (Stripe, n.d.).

Instant digital payment systems **reduce the risk to a seller of non-payment**, as the payment cannot be reversed. However, this feature also **increases the risk of loss to investors and buyers** through scams and fraud, where financial and other products and services are promised

but never delivered. This requires consumers to be particularly vigilant.

Forging ahead

South Africa’s journey towards truly instant and inclusive payment systems is exciting, offering unparalleled convenience and efficiency. However, it is fundamentally intertwined with the critical responsibility of protecting our personal data.

Through comprehensive legislation like POPIA, alongside advanced security measures such as encryption and tokenisation, we can work towards a future where fast digital payments are not only seamless, but also inherently private and secure. It's about building trust in a rapidly evolving digital economy.

References

- Baker McKenzie. (2025, May 8). *South Africa: Amendments to the POPIA regulations – Key changes you need to know*. Retrieved from https://connectontech.bakermckenzie.com/south-africa-amendments-to-the-popia-regulations-key-changes-you-need-to-know/
- Bank for International Settlements (BIS). (2025, January 23). *Privacy-enhancing technologies for digital payments: mapping the landscape*. Retrieved from https://www.bis.org/publ/work1242.pdf
- Chargeflow. (n.d.). *Challenges of Digital Payment and Prevention Strategies*. Retrieved from https://www.chargeflow.io/blog/challenges-of-digital-payment-and-prevention-strategies
- GDPR.eu. (n.d.). *GDPR and Payments: A Guide to Data Protection Compliance*. Retrieved from https://gdprlocal.com/gdpr-and-payments/
- G2 Learning Hub. (2025, February 4). *10 Best Practices To Measure Payment Processing Security*. Retrieved from https://learn.g2.com/payment-processing-security
- Juspay. (n.d.). *The Impact of GDPR on Payment Data Handling*. Retrieved from https://juspay.io/blog/impact-of-gdpr-on-payment-data-handling
- Michalsons. (n.d.). *Consent, POPI and other legal requirements*. Retrieved from https://www.michalsons.com/blog/consent-popi-and-other-legal-requirements/12623
- PayFast. (n.d.). *What is POPIA and how does it affect your online business?* Retrieved from https://payfast.io/blog/what-is-popia-and-how-does-it-affect-your-online-business/
- POPIA. (n.d.). *Protection of Personal Information Act (POPI Act)*. Retrieved from https://popia.co.za/ (Specifically referencing Sections 11, 19, 20, 22, 23-25, 105, 106)
- SimplePay. (n.d.). *POPIA*. Retrieved from https://www.simplepay.co.za/popia
- Square. (n.d.). *Payment Tokenization Explained*. Retrieved from https://squareup.com/us/en/the-bottom-line/managing-your-finances/what-does-tokenization-actually-mean
- Standard Bank. (n.d.). *A guide to POPIA*. Retrieved from https://www.standardbank.co.za/southafrica/personal/learn/everything-you-need-to-know-about-popia
- Stripe. (n.d.). *Payment security explained: A guide for businesses*. Retrieved from https://stripe.com/gb/resources/more/payment-security
- SurePay. (n.d.). *Understanding the EU Instant Payments Regulation (IPR): What banks need to know*. Retrieved from https://www.surepay.eu/understanding-the-eu-instant-payments-regulation-ipr-what-banks-need-to-know/
- World Bank. (n.d.). *CYBER RISKS IN FAST PAYMENT SYSTEMS*. Retrieved from https://fastpayments.worldbank.org/sites/default/files/2025-02/Cybersecurity%20Focus%20Note_Feb%2019_Final.pdf
- Worldpay. (n.d.). *What is payment tokenization and how does it work?* Retrieved from https://www.worldpay.com/en/insights/articles/what-is-tokenization-how-it-works