

EASYEQUITIES CYBER BREACH: IS YOUR PERSONAL INFORMATION SAFE?

Category: Privacy Law and POPIA, Privacy Law, Infosec, and POPIA
written by Tshimangadzo Nengovhela | October 5, 2026



The recent cybersecurity incident affecting EasyEquities has raised significant concerns regarding the protection of customer personal information, third-party vendor risk management, and regulatory compliance within South Africa's financial services sector. According to public disclosures, the incident appears to stem from a breach involving a third-party identity verification and compliance service provider rather than a direct compromise of EasyEquities' own systems. EasyEquities has stated that its internal investigation found no evidence that its trading platform or customer accounts were compromised.

While the full scope of the incident remains under investigation, the event raises important legal questions under the *Protection of Personal Information Act, 2013* ("**POPIA**"),^[1] the *Financial Intelligence Centre Act* ("**FICA**"),^[2] and the regulatory framework overseen by the Information Regulator and the Financial Sector Conduct Authority ("**FSCA**").^[3]

In communications to customers, EasyEquities disclosed that a third-party service provider used for customer verification processes experienced a cybersecurity incident that may have affected customer information.^[4] The verification provider reportedly performs identity and compliance checks required for regulatory obligations, including Know Your Customer ("**KYC**") and anti-money laundering compliance.

Several reports indicate that the affected third-party provider may be Rely Comply, a compliance platform used by multiple South African financial institutions for FICA verification processes. Reports

suggest that the potentially exposed information may include:

- Full names
- Identity numbers
- Passport numbers
- Dates of birth
- Contact information
- Residential addresses
- Banking information

The exact extent of unauthorized access remains subject to ongoing forensic investigation.

Importantly, EasyEquities has stated that customer funds remain secure, trading systems were not breached, and user credentials and account functionality were unaffected.

However, the investigation remains ongoing.

The primary legislation governing this incident is POPIA. Under POPIA, EasyEquities acts as a “Responsible Party” for customer information, even when external operators or service providers process data on its behalf.[\[5\]](#) The use of third-party vendors does not eliminate the duty to protect personal information. POPIA requires companies to maintain appropriate technical and organisational security measures, identify reasonably foreseeable risks, verify that third-party operators implement adequate safeguards, and take immediate action following a security compromise.[\[6\]](#)

Regulatory Steps That Are Required to Happen

Step 1: Conduct a Forensic Investigation

The first legal requirement is a comprehensive forensic investigation to determine whether personal information was accessed, what categories of information were affected, how the access occurred, the number of affected individuals, and whether the information was copied, exfiltrated, altered, or destroyed.[\[7\]](#) EasyEquities and the third-party provider have already indicated that forensic investigations are underway.

Step 2: Notify the Information Regulator

Section 22 of POPIA requires that the Information Regulator be notified whenever there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorized person.[\[8\]](#) The notification must contain a description of the incident, the categories of personal information affected, the measures that have already been implemented to address the compromise, and recommendations for affected individuals. This notification must be submitted as soon as reasonably possible after the compromise has been discovered.

Step 3: Notify Affected Customers

If there is a reasonable belief that personal information has been compromised, affected customers must be informed directly. The notification should clearly explain the nature of the breach, identify the types of information that may have been affected, outline any potential risks arising from the incident, and provide guidance on protective measures that customers should take. These measures may include monitoring account activity, remaining vigilant for phishing or other fraudulent communications, replacing potentially compromised credentials, and enabling multi-factor

authentication where available. EasyEquities has already taken steps to mitigate potential harm by issuing precautionary warnings to customers regarding suspicious communications.

Step 4: Assess Third-Party Operator Compliance

POPIA requires responsible parties to ensure that any operators processing personal information maintain appropriate security safeguards to protect that information. Following a security incident, a comprehensive review should be conducted to evaluate the adequacy of vendor cybersecurity controls, compliance with contractual obligations, data retention practices, encryption standards, and incident response capabilities. This assessment helps determine whether existing safeguards were sufficient and identify any weaknesses that may have contributed to the incident. Where deficiencies are identified, it may be necessary to implement contractual, technical, and operational remediation measures to strengthen security and ensure ongoing compliance with POPIA requirements.

Step 5: FSCA and Financial Sector Reporting

Because EasyEquities operates within the regulated financial services sector, the incident may give rise to obligations under the financial regulatory framework overseen by the FSCA. In such circumstances, the FSCA may require the reporting of the incident, the performance of governance reviews, assessments of operational resilience, evaluations of the effectiveness of cybersecurity controls, and confirmation that customer impact assessments have been conducted. These requirements reflect the broader expectation that financial institutions maintain strong cybersecurity governance, effective risk management practices, and resilient operations to safeguard customers, preserve market integrity, and ensure the continued stability of the financial services environment.

Step 6: Risk Mitigation and Remediation

Following the findings of the investigation, EasyEquities may be required to implement a range of corrective measures to address identified weaknesses and strengthen its overall security posture. These measures may include enhanced monitoring of third-party vendors, improvements to existing security controls, stronger encryption practices, the implementation of additional data loss prevention mechanisms, and more robust identity verification processes. In addition, EasyEquities may need to review and revise its cybersecurity governance framework to ensure that security risks are appropriately managed and monitored. Implementing these corrective actions is essential not only to reduce the likelihood of future incidents but also to demonstrate ongoing compliance with POPIA's accountability requirements and commitment to protecting personal information.

Potential Legal Consequences

If regulatory investigations reveal failures in data protection practices, several consequences may follow. Following a personal information compromise, the Information Regulator may exercise its enforcement powers by issuing enforcement notices, requiring specific remedial actions, conducting compliance investigations, and, where warranted, referring serious matters for prosecution. In addition to regulatory consequences, affected individuals may have the right to pursue civil claims if they suffer damages as a result of unlawful processing or the inadequate protection of their personal information. Beyond legal and regulatory exposure, EasyEquities may also face significant reputational risks. As a financial institution that depends heavily on customer trust and confidence, any disclosure or compromise of personal information can negatively affect its reputation, customer relationships, and public perception, even in circumstances where no direct financial losses are incurred by customers.

What Customers Should Do

Affected customers should take proactive steps to reduce the risk of fraud and identity theft following a potential compromise of personal information. Recommended measures include enabling multi-factor authentication on all relevant accounts, regularly monitoring investment and banking accounts for unauthorized activity, remaining vigilant for phishing emails, SMS messages, and phone calls, and changing passwords immediately if there is any reason to believe that login credentials may have been exposed. Customers should also monitor their credit profiles for indications of identity theft and report any suspicious activity to the relevant financial institution or authorities without delay. These precautions are particularly important where identity documents, KYC records, or other sensitive personal information may have been compromised.

The EasyEquities cyber incident appears to be a significant third-party supply-chain cybersecurity event rather than a direct compromise of EasyEquities' infrastructure. Nevertheless, under South African law, the company remains accountable for ensuring that personal information entrusted to service providers is adequately protected.

From a regulatory perspective, the key next steps include completion of forensic investigations, notification of the Information Regulator where required, communication with affected customers, assessment of third-party compliance failures, and potential oversight by the FSCA. The ultimate legal exposure will depend on the findings regarding what information was accessed, the adequacy of security safeguards in place, and whether all statutory breach-notification obligations were satisfied.

[1] *Protection of Personal Information Act, of 2013.*

[2] *Financial Intelligence Centre Act, of 2001*

[3] Financial Sector Conduct Authority, *Conduct Standard for Banks and Financial Institutions on Cybersecurity and Cyber Resilience*, various publications and guidance notes.

[4] EasyEquities, Customer Security Incident Notice, September 2026.

[5] Section 19, Protection of Personal Information Act, of 2013.

[6] Section 22, Protection of Personal Information Act, of 2013.

[7] Information Regulator South Africa, *Guidance Note on Security Compromises and Data Breach Notifications*, available at: <https://www.justice.gov.za/inforeg> (Accessed: 28 September 2026).

[8] Section 22(1)-(4), Protection of Personal Information Act, of 2013.