

FUNDS PROTECT BUSINESS POLICY

A QUICK AND CONCISE GUIDE TO OUR PRODUCT AND HOW WE HELP SECURE YOUR BUSINESS FUNDS



WHAT IS COVERED



A loss of funds



from an account in the name of your business



as a result of a Funds transfer



whether authorised or unauthorised



due to the fraudulent conduct of a third party



which is irrecoverable from your financial institution or third party

WHO IS THIS PRODUCT SUITABLE FOR?



Any business that holds a bank account or similar account



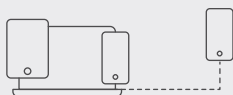
Any business that transacts online



Any business that pay vendors via EFT

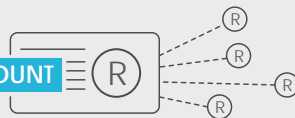
KEY CONCEPTS

ACCESS DEVICE



The device used to transfer funds e.g computer, mobile phone etc

ACCOUNT



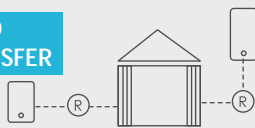
Bank account in the name of your business used for business transactions

FINANCIAL INSTITUTION



Your Bank

FUND TRANSFER



An electronic transfer of funds from your account for a business transaction

INTERNET SECURITY



Up to date and paid for licensed internet security software in the name of your business

LOSS OF FUNDS



Actual monetary amount debited from your business account due to fraudulent conduct of a third party. Includes amounts paid for cyber extortion events (see limitations)



UNDERWRITTEN BY

+27 (010) 312 5257 enquiries@phishield.com www.phishield.com
Fourways View Office Park, Block C, 1210 Sunset Ave, Fourways, 2055



CONDITIONS OF COVER



- All access devices must be protected by internet security software
- Payment of the premium in advance

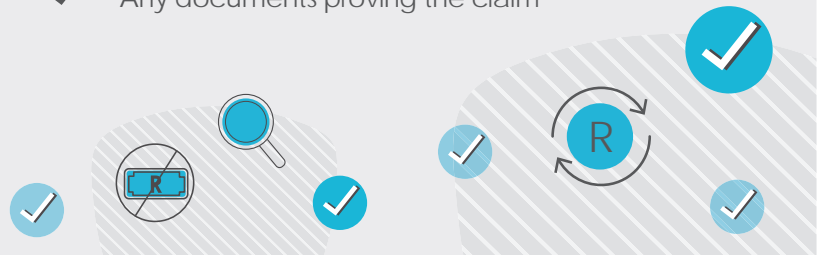
MAJOR FEATURES



- Ⓞ **Authorised and unauthorised funds transfers are covered**
- Ⓜ **Affordable**
- ✓ **Simple application process**
- 😊 **Easy claims procedure with no excess payable**

NEED TO CLAIM – NOW WHAT?

- Within 24hrs of becoming aware of the loss, notify your financial institution to avoid further transactions
- Lodge a claim with Phishield within 90 days of Funds Transfer date by submitting
 - ✓ Fully completed claim form
 - ✓ Bank statement reflecting the Funds Transfer
 - ✓ Letter from bank stating that they will not reimburse the loss
 - ✓ Company registration documentation or related documents
 - ✓ Any documents proving the claim



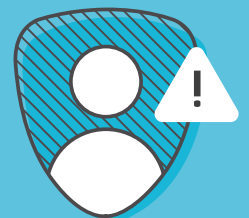
EXAMPLES OF EVENTS (not an exhaustive list)

- Email interception fraud
- Transactions due to your business's stolen identity
- EFT/deposit scams
- Hacking /phishing/vishing attacks
- Demands for ransomware attacks, denial of service attacks etc
- Sim Swap fraud
- EFT Fraud
- Online banking fraud
- Online shopping fraud
- Accommodation booking scams
- Bogus property rentals
- Fraudulent invoices



LIMITATIONS

- Payments made in cash
- Cyber extortion losses are limited to 10% of the cover limit
- Losses of funds transfer prior to inception date
- Funds Transfer effected by your financial institution
- All transactions with a common cause are treated as one event
- Personal transactions
- Employee's financial losses



WHAT IS NOT COVERED

- ✗ Fraudulent/dishonoured cheques
- ✗ **Trust Accounts such as held by Legal Practitioners and Estate Agents**
- ✗ Errors/omissions/negligence
- ✗ Losses due to a loss of goods
- ✗ Dishonest, criminal, malicious, fraudulent acts by your employee
- ✗ Transactions deducted /reversed by your financial institution
- ✗ Cryptocurrency accounts /unregulated funds or schemes
- ✗ Inter-company/subsidiary business funds transfers
- ✗ Losses due to non delivery of goods/services
- ✗ Goods/services advertised on classified sites

