GARRUN COVER FOR PROFESSIONALS

WHEN MONEY GOES MISSING:
WHY "WHICH POLICY RESPONDS?" IS NEVER A SIMPLE QUESTION

Written by Lauren Anderson and Noleen Podrouzek

When money disappears from a business, the instinct is to look for the nearest policy that mentions fraud, hacking or theft and assume the claim will fall neatly into place.

In reality, financial crime losses rarely follow neat lines.

Commercial Crime, Fidelity Guarantee, Cyber Liability and Trustees Liability all use overlapping language. Add to this the fact that policy wordings differ materially between insurers and underwriting managers, and the complexity multiplies. What one product includes as standard, another may only offer by extension — or exclude altogether. This is where broker responsibility becomes critical.

Understanding a client's operations, how money flows through their business, where internal controls sit and how digital systems interact with banking platforms is just as important as understanding the wording of the policy being recommended. When money goes missing, assumptions are expensive.

It is also important to understand that these policies do not respond automatically simply because fraud or theft has occurred. Most Commercial Crime and Cyber policies are built around specific conditions and minimum control requirements. These often include measures such as dual authorisation for payments, segregation of duties, secure credential management, verification procedures for banking changes, regular reconciliation of accounts and documented internal controls. Insurance is designed to transfer risk — not replace basic operational discipline. Businesses remain responsible for taking reasonable care to protect their money, systems and processes. Where required controls are not in place or have been consistently ignored, this can materially affect a claim outcome.

Let's unpack some of the most common real-world scenarios and explore how different policies may respond — and why the "best" answer is rarely as simple as it first appears.

When the Trusted Employee Becomes the Risk

Imagine a long-serving bookkeeper who slowly diverts money from the company account. Small EFT payments go unnoticed for months. Nothing dramatic. Nothing obvious. By the time the fraud is uncovered, the loss is substantial. This is one of the most common financial crime claims in South Africa.

In most modern placements, Commercial Crime has become the strongest primary solution for theft and fraud exposure — provided it is correctly structured and matched to the client's risk profile. These policies are designed to insure direct financial loss caused by dishonest or fraudulent acts of employees and typically offer broader protection than traditional fidelity products. They are better suited to electronic payments, modern banking environments and complex internal fraud scenarios.

That said, Fidelity Guarantee can also respond to this type of loss. Historically, it was the standard solution for employee theft. However, it is generally narrower in scope, often more restrictive in structure and less adaptable to electronic crime. This does not make Fidelity "wrong", but it does make Commercial Crime the more robust primary option where available.

What matters most is not the product name on the schedule. It is whether the policy being placed actually reflects how the client handles money in practice.

When Payroll Fraud Looks Like Cyber Crime (But Isn't)

Now consider a different scenario. A payroll manager creates fictitious employees and diverts salary payments into a personal account. The fraud is executed through payroll software.

Because technology is involved, this often gets misclassified as cyber risk.

In reality, the trigger is not hacking. There is no unauthorised access. The employee already had legitimate system permissions. The computer system is simply the tool used to commit the fraud, not the cause of the loss.

This remains an employee dishonesty claim.

Commercial Crime remains the best primary solution here because it is built to handle internal fraud and electronic misuse by authorised staff. Fidelity-type cover may also respond, depending on the wording, but with similar structural limitations as discussed earlier.

Cyber Liability, however, is usually not the correct policy for this scenario. It is designed to respond to network breaches, unauthorised access and security failures — not internal abuse of legitimate credentials. While some hybrid Cyber products now include limited internal fraud or theft-of-funds extensions, these remain highly conditional and are not designed to replace specialist Crime cover.

This distinction may feel technical, but it is fundamental to correct placement.

When Hackers Empty the Bank Account

Now picture a more dramatic event. A finance employee falls victim to a phishing email. Login credentials are compromised. Fraudsters initiate unauthorised EFT payments and drain the company's bank account overnight.

At first glance, this feels like a cyber claim — and operationally, it often is. There may be forensic investigations, system reviews and urgent security remediation.

But the insured loss itself is not only the phishing email or system breach - It is the theft of money from the company's bank account.
This is where Commercial Crime remains the primary financial protection. These policies are specifically designed to insure fraudulent banking instructions, electronic funds transfer theft and external criminal activity targeting company accounts.

Cyber Liability may support the response by covering forensic work, breach management and regulatory engagement. Some Cyber policies also offer theft-of-funds extensions. However, these are optional, sub-limited and highly conditional. They are not designed to replace proper Crime cover.

Cyber may manage the crisis. Commercial Crime pays for the stolen money (subject to compliance with policy conditions and internal control requirements)

When Trust Money Is Involved

Now consider a different environment altogether. A trustee misappropriates funds from a formal trust account. Beneficiaries suffer financial loss and legal action follows.

Here, the issue is no longer simply theft.

It is fiduciary responsibility.

Trustees Liability policies exist specifically to protect trust structures, trustees personally and beneficiaries' financial interests. They often include dedicated extensions addressing misappropriation and fraud within fiduciary environments.

Commercial Crime and Cyber Liability are not substitutes for this exposure. They were never designed to insure governance failure or breach of trust obligations.

This is not layering — it is specialist placement.

Understanding How These Covers Actually Work Together

Commercial Crime and Cyber Liability form the core operational protection for most modern businesses. One is designed to insure the theft of money and property. The other is designed to insure digital incidents, data breaches and the fallout from cyber events. Together, they address the financial and technological risk landscape that most organisations now operate within.

Fidelity Guarantee sits in the same risk category as Commercial Crime — but it does not sit on the same level.

Commercial Crime was developed specifically to improve on the limitations of traditional Fidelity Guarantee products. Where Fidelity Guarantee historically focused on basic employee theft, Commercial Crime was designed to be broader, more flexible and better suited to modern banking, electronic payments and sophisticated fraud methods.

In many placements today, Fidelity Guarantee no longer exists as a standalone solution. It often appears as a narrow extension within standard commercial policies, with tighter conditions and more exclusions. Commercial Crime, by contrast, is structured as a specialist product, offering wider theft protection, stronger electronic crime cover and more robust claims support mechanisms.

For this reason, where Commercial Crime is correctly structured and placed, standalone Fidelity Guarantee is usually unnecessary. It is not a complementary layer — it is a more limited alternative.

Trustees Liability remains separate from this discussion. It does not compete with Commercial Crime or Cyber Liability. It exists to protect formal trust structures and fiduciary responsibility and should only be introduced where those legal arrangements exist.

This is not about stacking policies. It is about designing protection that reflects how money, data and responsibility actually flow through a business.

The Reality Brokers Cannot Ignore

When money goes missing, it is rarely just a financial shock. It disrupts operations, damages trust, consumes management time and creates enormous emotional strain. In those moments, the last thing any business owner wants to discover is that the wrong type of insurance was in place.

The reality is that not all “fraud” or “cyber” losses are the same. Internal theft, electronic banking scams, payroll fraud and data breaches trigger different types of insurance cover — even when they appear similar on the surface. What matters is not only what happened, but how it happened, who was involved and what the actual loss was.

This is why choosing the right insurance structure upfront is so important.

It is not about buying more policies. It is about making sure the right protection is in place for how your business actually operates — how money moves through your accounts, how payments are authorised, how data is stored and how responsibility is shared internally.

Specialist brokers exist for this reason.

Our role is not simply to arrange cover. It is to understand your risk environment, identify where financial and digital exposures sit, and structure protection that works together when something goes wrong. That includes making sure Commercial Crime, Cyber Liability and other specialist covers are correctly positioned — not duplicated, not assumed, and not misunderstood.

Because when money goes missing, the quality of your advice partner matters just as much as the policy itself.

And the right structure, put in place early, can make all the difference.

When money goes missing, the outcome is often decided long before a claim is submitted.

It is decided when the broker chooses which policies to place, which extensions to include, what limits to recommend, and how clearly coverage is explained to the client. It is decided by whether the wording was read, understood and matched to the client’s real-world operations.

Financial crime placement is no longer a box-ticking exercise. It is risk architecture.

And in a world where fraud is increasingly sophisticated, digital crime is accelerating and regulatory pressure continues to rise, that responsibility has never been greater.

The real value of a broker is not in selling policies.

It is in building protection that still works when everything goes wrong.

Need Insurance – Contact Us

It’s quick and easy, you can apply for cover online:

https://cover4profs.co.za/cyber-liability-insurance/

Send us a WhatsApp on: 076 284 8108 **Phone:** 011 794 6848 **Email:** specialists@garrun-group.co.za

Authorised Financial Service Providers; FSP 25426