ICTS
LEGAL SERVICES

Cyber news that bites back

Issue 11 • October 2026

WHAT THE HACK?



NEWS

BLACK OCTOBER: WHEN DEFENCES THAW

Cybersecurity briefing for South African retirement fund trustees, Principal Officers and their providers

HACK HAPPENINGS IN OCTOBER

FSCA CLARIFIES JOINT STANDARD 2 – KEY POINTS FROM 27 OCTOBER WEBINAR

BINANCE – THE LARGEST CRYPTO THEFT ON RECORD



HOT OFF THE PRESS

BINANCE – THE LARGEST CRYPTO THEFT ON RECORD

What happened: Late on Thursday 29 October the world's biggest cryptocurrency exchange, Binance, was hit by what is already being called the largest single crypto theft in history. Roughly $6.3 billion (some analysts put the figure at $6.36 billion) in digital assets was drained from the exchange's internet-connected "hot wallets" – the wallets it uses for everyday customer withdrawals. The money left across about nine to ten different blockchains (Bitcoin, Ethereum, Tron, Solana, XRP Ledger and others). Most of it moved in a remarkably short window of about 20 minutes. On Ethereum alone, one large transfer swept away more than 167,000 ETH plus over $1.6 billion in USDT and dozens of other tokens. Binance's early investigation pointed to a compromised laptop belonging to a DevOps engineer. That single device gave the attacker a way into an internal service that is allowed to request withdrawals. Importantly, there was no evidence that the actual private keys controlling the wallets had been stolen; the attacker simply used legitimate access paths that the compromised laptop opened. Preparation appears to have started at least a day or more earlier.

Who was behind it: Binance itself has not named a perpetrator. However, two leading blockchain analysis firms – TRM Labs and Chainalysis – have attributed the attack with high confidence to North Korea's elite hacking unit TraderTraitor (part of the broader Lazarus Group). This is the same type of state-linked group the FBI blamed for the previous record $1.5 billion theft from the Bybit exchange in February 2025. The pattern matches earlier North Korean operations: careful preparation, use of privacy tools to fund the attack, and a sudden, highly coordinated burst of withdrawals across many networks. North Korean groups have a long track record of stealing crypto to fund the regime's weapons programmes.

How they responded: Binance suspended all deposits and withdrawals within hours while it investigated and secured its systems. It publicly stated that customer funds were safe and that it would cover every loss from its Secure Asset Fund for Users (SAFU) emergency reserve plus the company's own money. Industry partners moved extremely quickly. Tether froze roughly $1.5–1.6 billion in USDT, Circle froze more than $800 million in USDC, and other issuers (Ripple, World Liberty Financial, Arbitrum's Security Council and others) locked further amounts. In total, about $2.7–3 billion was frozen on-chain within hours. Bitcoin and Ethereum cannot be frozen by an issuer in the same way, so a large portion remained with the attacker. The attackers also raced the freezes by quickly swapping some stablecoins for other assets before the locks took effect. Binance said it was working closely with law enforcement and blockchain investigators and would publish a full technical post-mortem once the facts were verified. Deposits were later reopened; withdrawals remained paused while security checks continued, with a target of restoring them within about 48 hours.

Impact: At $6.3 billion this is roughly four times larger than the previous record (Bybit 2025). About half the funds were frozen relatively quickly; roughly $3.1–3.3 billion remained with the attacker at last count, mostly in Bitcoin (around 18,270 BTC split into 19 wallets) and Ethereum that cannot be easily clawed back. Markets reacted immediately – Bitcoin fell several percent and related stocks such as Coinbase also dropped. The incident showed that even the largest, best-resourced platforms can lose enormous sums when a single privileged employee device is compromised. For Binance's customers the practical impact was temporary inability to withdraw, but the exchange's pledge to make everyone whole using its own reserves limited direct member losses. Wider confidence in crypto was shaken again.

Lesson for trustees: The entry point was not a clever new flaw in the blockchain itself. It was a compromised staff laptop that gave access to systems allowed to move money. This is a classic privileged-access and insider-device problem. Boards should ask every critical service provider (administrators, insurers, custodians, asset managers, payment platforms): how do you protect the devices and accounts of people who can authorise large movements of money or data? What multi-factor controls and monitoring sit around those privileged accounts? What happens if one of those devices is taken over? How quickly can you detect, freeze or recover assets? And do you have the reserves or insurance to make members whole if something goes wrong? The same questions apply whether the provider is a crypto exchange, a traditional fund administrator, or an insurer. Joint Standard 2 expects boards to oversee third-party cyber risk properly and to have clear incident-response arrangements.



OCTOBER'S COLD SNAP FOR CYBER DEFENCES

October 2026 was a rough month for organisations that hold other people's money or personal information. Several high-profile incidents showed how quickly a digital problem can become a real loss of money, trust or personal data. This edition looks at what actually happened in plain language, what the organisations did about it, and what trustees can learn.

For retirement fund boards the message is direct: Joint Standard 2 of 2024 is not a paperwork exercise. On 27 October the FSCA used a practical webinar to spell out what "reasonable" oversight actually looks like. We also explain the dark web simply, summarise the FSCA's guidance, and highlight the new ICTS Academy course.



HACK HAPPENINGS IN OCTOBER

GUARDIAN'S FUND – MONEY MEANT FOR VULNERABLE PEOPLE WAS REDIRECTED

What happened: The Guardian's Fund holds money for minors, missing persons and other people who cannot manage their own affairs. In late September 2025, someone changed the bank account details of legitimate beneficiaries on payment lists at the Pietermaritzburg and Makhanda offices. About R13.5 million was paid into fraudulent accounts instead of the rightful recipients.

Who was affected: Vulnerable beneficiaries and the Department of Justice and Constitutional Development, which administers the Fund.

How they responded: The fraudulent accounts were frozen the same day. A criminal case was opened, laptops were seized for investigation, and the Asset Forfeiture Unit was brought in. Most of the money had already been withdrawn, so recovery has been very limited.

Impact: R13.5 million lost. Public confidence in a system that exists to protect the vulnerable was damaged. Payments were disrupted while investigations continued.

Lesson for trustees: Changing bank details is one of the oldest and most effective fraud methods. Boards must insist that administrators have strong checks (two people must approve changes) and that those checks are independently tested. Accountability cannot be outsourced.

PHP PROBLEM – THOUSANDS OF WEBSITES SUDDENLY BECAME EASY TO BREAK INTO

What happened: PHP is the software that runs a huge number of websites and online forms around the world (including many member portals). In October, two serious weaknesses were discovered that let outsiders take control of a website without needing a password. The problems were so serious that details leaked before the fix was ready, and attackers started trying to exploit them immediately.

Who was affected: Any organisation whose website or online system uses PHP – including government sites, banks, insurers and service providers. South Africa's Presidency website was taken offline as a precaution. Thousands of South African servers were at risk.

How they responded: PHP released emergency fixes on 21 October. Organisations and hosting companies scrambled to apply the updates and restart their systems. Some took websites offline until they could be sure they were safe.

Impact: Widespread risk of websites being taken over, data stolen or systems disrupted. Many organisations had to drop everything to patch. The speed of the response determined who stayed safe.

Lesson for trustees: Ask your administrators and service providers a simple question: "Do any of our member websites or portals use PHP, and have they been updated and restarted?" A policy that says "we patch" is not enough – you need evidence that it was actually done.



RAND MUTUAL ASSURANCE – CLAIMS DATA PUT UP FOR SALE

What happened: In late October, Rand Mutual Assurance (a major South African insurer that handles occupational injury and disease claims) was alerted to possible unauthorised access to its systems. A criminal group claimed to have stolen a large volume of data – roughly 1.68 million claims records plus hundreds of thousands of supporting files – and demanded a ransom of about R1.5 million to keep it private.

Who was affected: Rand Mutual Assurance and the people whose claims information may have been taken (potentially including medical details and identity documents).

How they responded: The company confirmed it was investigating with specialist teams and said it would communicate further once it knew more. At the time of writing the investigation was still ongoing.

Impact: Risk of sensitive personal and medical information being sold or misused. Reputational damage and potential regulatory obligations under POPIA if personal information was compromised.

Lesson for trustees: Claims and medical data are extremely valuable to criminals. Funds must have clear, enforceable timelines in contracts so that administrators and insurers tell them quickly when something goes wrong – not just "as soon as possible."

AMPATH LABORATORIES – PATIENT INFORMATION COMPROMISED

What happened: Ampath, one of South Africa's largest pathology laboratories, confirmed it had been attacked. A criminal group claimed to have copied large amounts of patient, employee and financial data and threatened to release it. Ampath acknowledged that personal information and medical-aid details were likely affected, although it disputed the full scale of the claim.

Who was affected: Patients who had used Ampath's services, as well as the laboratory itself.

How they responded: Ampath confirmed the incident publicly and began assessing what data had been accessed. The criminal group publicised the claim on underground forums to increase pressure.

Impact: Personal and medical information at risk of misuse. Potential for targeted fraud against patients and further damage to trust in the health sector.

Lesson for trustees: Health-related data linked to members can be used for very convincing scams. Boards should ask providers whether they monitor for their data appearing on criminal marketplaces and how they would notify the fund if it did.



SUPERMARKET FREEZERS TURNED INTO OVENS

What happened: Attackers gained access to the refrigeration control systems of hundreds of supermarkets in France (and some in other European countries). They switched the freezers and cold rooms into continuous defrost mode. Temperatures rose to around 50 °C for several hours, destroying meat, dairy and frozen goods.

Who was affected: Multiple supermarket chains and their customers. Stock had to be thrown away.

How they responded: Stores discovered the problem when staff opened freezers in the morning and were hit by a wave of hot air. Food safety rules required them to discard anything whose temperature history could not be guaranteed. The manufacturer of the controllers issued alerts.

Impact: Significant financial loss from destroyed stock and operational disruption. The attack showed that connected equipment can be turned against its owners.

Lesson for trustees: Any system that can be reached from the internet (or from a compromised laptop) can be reconfigured to cause harm. Funds should know which of their service providers run internet-facing control systems and whether those systems are properly locked down.

BROADER PICTURE – LAW ENFORCEMENT STRIKES BACK, OTHER LARGE BREACHES CONTINUE

What happened: INTERPOL's Operation Serengeti III (results announced in October) led to 1 462 arrests across 21 countries, including South Africa. Authorities disrupted more than 10 000 criminal networks and recovered over USD 105 million. The operation targeted ransomware, email fraud, investment scams and other cybercrime. Elsewhere, Capcom confirmed that data linked to 11.7 million customer accounts had been exposed, and Quest Diagnostics disclosed unauthorised access to certain patient records.

Impact: Positive in the case of the arrests and recoveries; ongoing risk and cost in the case of the data breaches.

Lesson for trustees: The volume of incidents means "it won't happen to us" is no longer realistic. The practical response is to make sure contracts force quick notification, demand independent proof that controls work, and practise what the board will do on a bad day.



THE DARK WEB – WHERE STOLEN DATA GOES TO WORK

The dark web is a hidden part of the internet that ordinary browsers cannot reach. Criminals use it to sell stolen personal information (including pension and medical records), access to already-hacked systems, and tools for committing fraud. Once data is there, it is very hard to get it back. For funds, this means a single successful phishing email or an unpatched member portal can put member details in the hands of criminals within hours. Asking providers whether they watch for your data on these marketplaces is a reasonable question under Joint Standard 2.

FSCA CLARIFIES JOINT STANDARD 2 – KEY POINTS FROM 27 OCTOBER WEBINAR

On 27 October 2026 the FSCA hosted a practical webinar presented by Andile Mjadu. The summary below draws from the notes of Bianca Bekker, Legal Advisor, ICTS Legal Services.

Governance remains the foundation

Cybersecurity is a board-level responsibility that cannot be outsourced. Roles must be clear and there must be independence between the people who run systems and the people who check them. Cyber risk deserves the same attention as investment and liquidity risk.

Third-party oversight

Simply saying "tell us if something happens" is no longer enough. Contracts need clear deadlines for notification. Where possible, funds should secure the right to independent checks. Even a fund with no systems of its own must still oversee the providers it depends on.

Basic hygiene is non-negotiable

Funds and their providers must have a documented strategy that is actually used. Essential practices include controlling who can access systems, requiring more than a password to log in, limiting what people can do, and keeping records of activity.

When something goes wrong

The fund should quickly know what is affected, who depends on it, and how serious the disruption is. Communicate early and clearly with members. Independent proof that controls work is required. Practising a bad day (tabletop exercises) helps show the board acted reasonably.

FSCA KEY TAKE-AWAYS AT A GLANCE

Area	What the FSCA expects
Governance	Board accountability cannot be outsourced. Clear roles and independent checks.
Hygiene	Control access, require more than a password, limit privileges, keep records.
Third parties	Clear notification deadlines; right to independent checks; understand concentration risk.
Incidents & assurance	Know the impact quickly; plain-language member communication; independent proof + practice runs.

SPECIAL SECTION: ICTS ACADEMY LAUNCHES V2 2026 COURSE



Cybersecurity and Cyber Resilience for Retirement Funds – Version 2 2026

ICTS Academy has launched the updated Cybersecurity and Cyber Resilience for Retirement Funds V2 2026 course. Building on the earlier version that explained Joint Standard 2, the new course focuses on how boards can identify the real risks their fund faces and what practical steps reduce those risks.

It is designed to support the annual trustee training that the Standard expects. Participants learn how to ask better questions of administrators, read assurance reports, and run meaningful practice exercises for a bad day.

For course dates and enrolment contact Toni at *cantint@icts.co.za*

LET'S PLAY ..... HACK OR MYTH?

Circle your answer. Answers below – no peeking.

1. **A fully outsourced fund has no cybersecurity obligations because it has no systems of its own. Hack / Myth**
2. **"Tell us if something happens" is still an adequate contractual clause. Hack / Myth**
3. **A letter from an administrator saying "we are secure" is enough if the board files it. Hack / Myth**
4. **Trustees who only log in occasionally do not need extra login protection. Hack / Myth**
5. **The dark web is just a myth used by ICTS Legal Services to scare boards. Hack / Myth**

Closing Thought

October showed that problems do not wait for boards to finish their paperwork. The FSCA has made clear what good looks like: the board owns the risk, basic controls must actually work, contracts must force quick notification, and the board must be able to show it asked the right questions and have practised for a bad day.

The ICTS Academy V2 course exists so that annual trustee training keeps pace with those expectations. Use it, ask the hard questions, and rehearse before the day arrives.

At ICTS Legal Services, we continue supporting pension funds, their providers, and trustees with compliance, assessments, risk management plans, training (ICTS Academy), and resilience strategies.

Questions or contributions? Contact us at ICTS Legal Services.

Sources for the Watch pages: company notices and ITWeb / MyBroadband / Moneyweb / Daily Maverick reporting 13–22 September 2026; RelyComply incident page 16 September 2026; MIP Holdings POPIA notice 23 June 2026; Comparitech ransomware round-up August 2026; FSCA Joint Standard 2 of 2024 and the Retirement Fund Supervisory Questionnaire Section 21. Assessment figures from the September 2026 provider-assessment snapshot supplied with this edition.

Contact
Leon Greyling
082 464 5786
greylingl@icts.co.za

Answers to Hack or Myth (and a bad joke)

1. Myth – Oversight cannot be outsourced.
2. Myth – Clear, enforceable deadlines are now expected.
3. Myth – Independent proof is required.
4. Myth – Extra login protection is basic hygiene for everyone with access.
5. Myth – The dark web is real, and stolen member data appears there regularly.



Joke of the edition:

Why did the trustee bring a USB stick to the board meeting?

Because the agenda said "plug the security gaps."
(Please don't. Ever.)



What The Hack is published monthly or when required. Past editions available on request.
This newsletter is for information purposes only and does not constitute legal advice.