

THE NEXT **\$50M+** SEIZED CRYPTO DISASTER IS COMING. WILL IT BE **YOURS?**



- Zero Seed Phrases
- 1-3 Day Recovery
- On-Chain Audit Trail
- Court-Ready

ZERO

No seed phrases to split, store, photograph, leak, coerce or steal

RAPID RECOVERY

On-chain workflows, often completed in 1-3 days

CYBER-READY

Designed for agencies, institutions & cybercrime teams

**BE THE UNIT THAT LEADS — NOT THE ONE
THAT EXPLAINS THE NEXT HEADLINE**
REQUEST DEMONSTRATION • zbselfbanking.com

CRITICAL DIGITAL ASSET CUSTODY PROTECTION BRIEF

Secure Custody & Rapid On-Chain Recovery for Seized, Stolen, Scammed or Lost Cryptocurrency

A GLOBAL LEADERSHIP OPPORTUNITY FOR CYBERCRIME OPERATIONS

ZERO

No seed phrases to split, store, photograph, leak, coerce or steal. The master secret is removed from the threat model entirely.

RAPID RECOVERY

Proven on-chain workflows for stolen, scammed or lost assets. Real recovery path, often completed in one to three days.

CYBER-READY

Built for agencies and cybercrime teams. On-chain verified identity, permanent records, court-ready accountability.

THE CURRENT MODEL HAS ALREADY FAILED — IN PUBLIC

South Korea NTS (Feb 2026): Officers published photos of seized wallets with handwritten seed phrase visible. USD 4.8M drained in hours.

U.S. Marshals (2025-26): Contractor's son allegedly stole USD 46M in seized crypto via insider access to wallets.

Splitting seed phrases only fragments the same dangerous secret. MYIDverified removes the master secret entirely and adds rapid on-chain recovery.

BE THE UNIT THAT LEADS — NOT THE ONE THAT EXPLAINS THE NEXT HEADLINE

WHY THIS MAKES THE AGENCY LOOK PREPARED

A cleaner custody model gives leadership a visible answer to the risks exposed in public failures.

01

PREVENT HEADLINE RISK

Remove seed phrases from the threat model before leaks, theft or insider misuse can become public damage control.

02

SHOW FASTER RESTITUTION

Move from slow, uncertain recovery toward actionable on-chain workflows that create a real path to victim outcomes.

03

EVIDENCE POSTURE

Tie identity, activity and records to verifiable on-chain actions so teams can defend decisions with confidence.

Outcome: better controls, stronger public-trust optics, and a clearer operational story for leadership.

REQUEST A SPECIALIST DEMONSTRATION & SECURITY ASSESSMENT

See live on-chain recovery turn historically unrecoverable losses into cases with a real path to restitution.

zbselfbanking.com

MYIDverified — Because digital assets require zero seed-phrase dependency and a real rapid on-chain recovery path.

MYIDverified for Cyber Crime Recovery Operations

Secure custody and rapid on-chain recovery: designed to eliminate seed-phrase dependency and provide a real recovery path for stolen, scammed or lost cryptocurrency, a category traditionally regarded as virtually impossible to recover through conventional methods.

A global leadership opportunity for cybercrime operations. MYIDverified gives agencies a modern, highly secure method to safeguard seized digital assets, protect victims and demonstrate the standard other agencies should follow in responsible crypto custody and recovery.

Zero

Seed phrases to split, store, photograph, leak, coerce or steal.

Rapid recovery

On-chain workflows for stolen, scammed or lost assets, often completed in one to three days.

Cyber-ready

Designed for agencies, institutions, cybercrime teams and digital-asset stakeholders.

The operational reality: any system that still creates, stores, splits, shares or reconstructs a seed phrase leaves a secret that can be known, copied, photographed, remembered, coerced, leaked, stolen or discovered later. For cybercrime, counter-scams, intelligence and digital-asset seizure stakeholders, MYIDverified eliminates that dependency and adds a decisive operational capability: rapid on-chain recovery when cryptocurrency has already been stolen, scammed away or lost.

General operating context

Cybercrime, online fraud, ransomware and digital-asset laundering affect agencies across English-speaking jurisdictions, including cyber-dependent crime such as ransomware and hacking, and cyber-enabled crime such as scams, cyber extortion and other online offences. Secure custody and rapid recovery require evidentiary integrity, accountable access and practical victim restitution.

The Problem

When cryptocurrency is seized, recovered, preserved for restitution or held as case evidence, custody must protect both the asset and the evidentiary record. Too many custody models still rely on a fragile master key: the seed phrase.

Splitting a seed phrase does not eliminate the threat. It only fragments the same dangerous secret. If the phrase was exposed at creation, copied before splitting, mishandled during documentation, accessed by a vendor or reconstructed later, the entire asset pool can still be compromised.

Traditional custody and investigation workflows were never built to recover crypto after theft, scams or loss. Once funds move, recovery is often treated as virtually impossible; MYIDverified changes that reality through verified identity, on-chain auditability and rapid recovery workflows.

The Risk Is Accelerating

- Cybercrime, scams, ransomware and laundering infrastructure increasingly intersect with digital assets.
- Funds can move instantly across borders, exchanges, mixers and obfuscation layers.
- More investigators, analysts, vendors and partner agencies can create more access points.
- Public loss of seized or recovered assets can become a headline event.
- Without a stronger custody layer, the next incident can be larger, faster and more visible.

Proof the Current Model Can Fail

DOCUMENTED DISASTER

South Korea National Tax Service — February 26, 2026

Officers reportedly published photos of seized hardware wallets with a handwritten seed phrase visible. Within hours, thieves drained **USD 4.8 million** in seized assets. A simple press photo allegedly destroyed months of enforcement work and forced public damage control.

INSIDER EXPOSURE

U.S. Marshals Service — 2025–2026

A government contractor’s son allegedly stole **USD 46 million** in seized cryptocurrency through insider access to wallets. Although tracing later identified a suspect, the episode exposed dangerous gaps in seized-asset management.

The Secure Operating Model: Zero Seed Phrases and Rapid On-Chain Recovery

MYIDverified is not positioned as another wallet, custodian or seed-splitting scheme. It is a patented, on-chain identity and recovery layer designed to protect custody and rapidly recover stolen, scammed or lost cryptocurrency when conventional methods no longer provide a practical path forward. This directly addresses vulnerabilities behind seed creation, seed splitting, photo leaks, historic exposure, external theft, weak auditability and insider misuse.

THE OLD, VULNERABLE WAY	MYIDVERIFIED — THE SECURE WAY	OPERATIONAL ADVANTAGE FOR CYBERCRIME STAKEHOLDERS
One seed phrase, or fragments of the same phrase, can be photographed, copied, reconstructed, leaked or stolen.	Seed phrases are eliminated rather than split, stored, distributed or later reconstructed.	Removes the original secret from the threat model and reduces internal or external theft risk caused by seed compromise.
Manual verification of rightful owners and claimants can be slow, opaque and document-heavy.	On-chain verified identity badges are tied directly to blockchain activity.	Supports faster, more transparent victim restitution, ownership verification and accountable asset handling.
Chain-of-custody records may be fragmented across teams, files, evidence stores and vendors.	Every action can be permanently recorded on-chain.	Creates stronger evidence, oversight and court-ready accountability across seizure, holding, review and disposition.
Recovery of stolen, scammed or lost crypto has traditionally been slow, uncertain or virtually impossible after funds move.	Proven on-chain recovery workflows are designed to provide a real recovery path, often completed in one to three days.	Moves the response model from post-incident investigation only toward rapid, actionable recovery and victim restitution.
Single points of failure may exist across officers, contractors, storage procedures and physical evidence practices.	Scam shielding and secure multi-staff verified controls reduce reliance on one individual or one exposed secret.	Enables safer long-term custody for seized funds, recovered assets, operational holdings and high-value case assets.

THE OPERATIONAL SHIFT

From fragile custody procedures to defensible recovery operations.

REMOVE

the single master secret from the agency risk model.

VERIFY

ownership, activity and case actions with on-chain records.

RECOVER

assets through workflows built for rapid restitution.

ZERO

SEED

PHRASE

DEPENDENCY

Why MYIDverified Is the Logical Upgrade for Digital-Asset Custody and Recovery

Effective cybercrime response emphasises coordinated capability, international cooperation and public-private collaboration. Secure digital asset custody must match that mission. MYIDverified is designed for the custody reality modern cybercrime divisions now face: no seed phrases to divide, no seed phrases to store, no seed phrases to reconstruct and no historic seed exposure waiting to be exploited later.

- ✓ **Prevent loss of seized or recovered assets** by eliminating the master secret most likely to be copied, photographed or misused.
- ✓ **Support cybercrime and scam investigations** with on-chain identity and activity linkage that can complement investigative workflows.
- ✓ **Enable rapid recovery of stolen, scammed or lost crypto** through on-chain workflows that can transform historically unrecoverable losses into actionable restitution cases.
- ✓ **Strengthen chain of custody** with on-chain action records, improved auditability and evidence continuity.

Secure Custody and Recover Stolen, Scammed or Lost Crypto

Request a specialist demonstration and security assessment. See how MYIDverified removes seed phrases from the custody threat model, then watch live rapid on-chain recovery turn losses once treated as virtually unrecoverable into cases with a real path to restitution.

[Visit zbselfbanking.com](https://zbselfbanking.com)

Secure what you seize. Protect victims.
Preserve evidence. Strengthen public trust.

A CLEAR PATH TO A BETTER STANDARD

Make the next briefing simple: demonstrate the model, map the workflow, and show leadership the operational advantage.

1 DEMONSTRATE

Show how custody operates without seed phrases to split, store, photograph or reconstruct.

2 MAP THE WORKFLOW

Connect seizure, verification, custody records and recovery activity into a defensible process.

3 BRIEF LEADERSHIP

Present a cleaner answer for victims, evidence integrity and public-trust protection.

THE MESSAGE TO THE AGENCY IS SIMPLE:

Secure what you seize. Recover what victims lost. Prove every action.

MYIDverified turns digital-asset custody from a reputational vulnerability into an operational advantage.