

Important Notice and Disclaimer

This document has been prepared for informational, research and illustrative purposes only. The case studies contained herein are based on information available through publicly accessible sources, including company statements, regulatory publications, law enforcement disclosures, security research and reputable media reporting. Veyns has not independently audited, investigated or verified the underlying incidents unless expressly stated otherwise.

Descriptions of cyber incidents may reflect preliminary findings, third party assessments or information available at the time of publication. The facts, attribution, financial impact, technical causes and conclusions associated with individual incidents may subsequently change as investigations progress or additional information becomes available.

References to Veyns within each case study are hypothetical assessments intended to illustrate how Veyns technology and human bound authorization architecture could potentially address specific authentication, identity or authorization risks demonstrated by the incident. Veyns was not deployed in, involved with or responsible for the systems discussed in these case studies unless expressly stated otherwise.

Statements regarding how Veyns could have prevented, mitigated or reduced the impact of an incident should not be interpreted as a guarantee that deployment of Veyns technology would have prevented the incident in its entirety. Cybersecurity outcomes depend on system architecture, implementation, configuration, operational controls, third party infrastructure, user behavior and the specific attack methodology involved.

Veyns is intended to complement, rather than replace, established cybersecurity controls, including secure software development, cryptographic key management, network security, access controls, hardware security, transaction monitoring, vulnerability management, fraud detection, governance and incident response.

No authentication or cybersecurity technology can eliminate all security, fraud, operational or privacy risks.

Any proposed deployment of Veyns within financial services, government, digital identity, digital assets, critical infrastructure or other regulated environments should be subject to appropriate technical validation, security assessment, legal and regulatory review, privacy impact assessment and integration testing prior to production use.

Company names, trademarks and product names referenced in this document remain the property of their respective owners. Their inclusion is solely for factual identification of publicly reported incidents and does not imply affiliation with, endorsement of, sponsorship by or partnership with Veyns.

This document does not constitute legal, regulatory, cybersecurity, investment or professional advice.

The Human Authentication Gap

22 real world incidents demonstrating the emerging limitations of passwords, keys, centralized biometrics and machine verifiable identity.

I. DIGITAL ASSETS & CRYPTOGRAPHIC AUTHORIZATION

1. Binance

6.3 billion digital asset theft | October 2026

Incident

On 29 October 2026, Binance suffered a compromise of its cryptocurrency hot wallet infrastructure, resulting in approximately $6.3 billion in digital assets being stolen through unauthorized withdrawals.

Binance's initial investigation indicated that a compromised DevOps engineer's laptop may have enabled attackers to access an internal service container and submit unauthorized withdrawal transactions. Subsequent investigations identified additional points of compromise. Binance reported no evidence of leaked wallet private keys, although the complete attack sequence remains under investigation. Binance Security Update

The incident demonstrates how compromised operational infrastructure can potentially enable unauthorized asset transfers without requiring direct theft of cryptographic private keys.

Control gap

The existing infrastructure failed to prevent unauthorized withdrawal requests from progressing through compromised internal systems.

The critical security concern is that access to operational infrastructure may provide a pathway to initiate financial transactions without sufficiently independent verification of the human authorizing the action.

Potential Veyns control

Veyns could introduce human-bound, transaction-specific authorization between internal withdrawal systems and the infrastructure responsible for executing asset transfers.

For high value withdrawals, Veyns could independently verify an authorized operator through palm-vein authentication and cryptographically bind that verification to the definitive transaction payload, including destination address, amount, blockchain network and operation.

This authorization would be enforced by an isolated signing system, preventing compromised laptops, service containers or operational credentials from independently authorizing asset movements.

If the transaction submitted for execution lacked valid human authorization or differed from the independently verified payload, the withdrawal would be rejected.

Potential outcome

The attacker would need to compromise not only Binance's internal infrastructure but also the independent human-authorization and transaction-signing controls.

If correctly implemented and enforced without bypass paths, Veyns could have blocked unauthorized withdrawals initiated through compromised infrastructure, potentially preventing or substantially limiting the financial loss.
Security principle: Authenticate the human. Authorize the transaction. Protect the assets.

2. Bybit

$1.46 billion digital asset theft | February 2025

Incident

On 21 February 2025, Bybit suffered a compromise of an Ethereum multisignature cold wallet resulting in approximately **$1.46 billion of digital assets being transferred**.
Subsequent forensic findings cited by Bybit concluded that credentials belonging to a Safe developer had been compromised, enabling unauthorized access to Safe infrastructure. Malicious code was then used to manipulate the transaction-signing experience and deceive legitimate Bybit signers into approving a transaction that altered the wallet's smart contract logic. Bybit
The incident is notable because the underlying authorization process already incorporated **cold storage, hardware wallets and multiple human signatories**.

Control gap

The cryptographic system could establish that valid keys had signed the transaction. The compromised workflow undermined the humans' ability to establish that the transaction being cryptographically executed was the transaction they intended to authorize.

Potential Veyns control

Veyns could introduce **human bound, transaction specific authorization** above the existing multisignature architecture.
For high value transactions, Veyns could locally verify an authorized operator and cryptographically bind that verification to the definitive transaction payload; including destination, amount, chain, contract and operation.
If the payload presented for execution differed from the independently verified payload, the human authorization would no longer be valid.
Potential outcome: the attacker would need to compromise not only the signing interface and credentials, but also obtain valid human authorization for the malicious transaction itself.
Security principle: Authenticate the action, not only the signer.

---

3. DMM Bitcoin

$308 million theft | May 2024

Incident

According to the FBI, North Korean actors targeted an employee of Japanese cryptocurrency wallet company Ginco through a fake recruitment approach and malicious Python coding exercise. Following the compromise, attackers obtained session cookie information, impersonated the employee and accessed Ginco's communications environment. The FBI states that the attackers likely used this access to manipulate a legitimate transaction request from a DMM Bitcoin employee.
The resulting transaction transferred **4,502.9 BTC, valued at approximately $308 million**, to attacker controlled wallets. FBI

Control gap

The attack demonstrates the risk of treating possession of a valid session or authenticated employee environment as sufficient evidence that subsequent activity represents the employee's legitimate intent.

Potential Veyns control

High risk wallet operations could require a **fresh human presence authorization**, independent of the employee's existing application session.

A stolen password, session cookie or compromised workstation would therefore not independently satisfy the transaction-authorization requirement.

Veyns could locally authenticate the authorized operator and generate a short lived cryptographic authorization restricted to the specific transaction.

Potential outcome: session compromise could still expose systems and communications, but it would not automatically provide authority to approve protected transactions.

Stealing the session should not mean stealing the human's authority.

---

4. WazirX

More than $230 million stolen | July 2024

Incident

WazirX reported that a cyberattack targeted an Ethereum multisignature wallet operated using Liminal's custody infrastructure.

The wallet contained **six signatories | five WazirX and one Liminal**. A normal transaction required approval from three WazirX signatories using Ledger hardware wallets followed by approval from Liminal.

Despite these controls, more than **$230 million** was stolen. WazirX

Control gap

Multisignature architectures increase the number of credentials required to authorize a transaction, but they remain dependent on the integrity of the systems presenting transactions to those signers.

Multiple valid signatures do not independently establish that multiple humans reviewed the same underlying transaction state.

Potential Veyns control

Veyns could extend multisignature into **human bound multisignature**.

Each authorized individual could be required to locally authenticate before signing, with each authorization cryptographically bound to the same immutable transaction hash.

A material change in destination, amount or contract execution would invalidate the collected human approvals.

Instead of establishing only:

Key A + Key B + Key C

the system could establish:

Verified Human A + Verified Human B + Verified Human C + identical transaction payload.

---

5. Ronin Network

173,600 ETH + 25.5 million USDC stolen | March 2022

Incident

Attackers obtained sufficient validator authority to authorize fraudulent withdrawals from the Ronin bridge.

The incident demonstrated a fundamental characteristic of private key infrastructure: once sufficient valid signing credentials are compromised, the underlying network may interpret the attacker's transaction as cryptographically legitimate.

Control gap

Cryptographic possession and human authorization are not the same thing.

A system can determine:

"This transaction contains a valid signature."

That does not necessarily establish:

"The authorized human knowingly initiated this transaction."

Potential Veyns control

For systemically important validator actions, Veyns could provide an additional **human authorization threshold**.

A validator key could remain operational for routine automated functions while extraordinary actions large withdrawals, validator changes or treasury movements require human bound authorization.

For example:

Validator Key + Policy Engine + Veyns Human Proof → Execution

Potential outcome: theft of validator credentials alone would not necessarily provide sufficient authority to execute protected operations.

---

6. Cetus Protocol

Approximately $223 million affected | May 2025

Incident

Cetus suffered an exploit involving vulnerabilities in its smart contract logic. Unlike the preceding incidents, the attack was not fundamentally dependent on impersonating an authorized individual or stealing that person's authentication credentials.

Control gap

This was primarily a **software and protocol security failure**, rather than an identity failure.

Potential Veyns control

Veyns would **not have prevented the underlying vulnerability**.

Human authentication cannot compensate for defective smart contract logic.

Veyns could nevertheless support secondary safeguards around privileged administrative actions, emergency intervention, treasury management and exceptional withdrawals.

This distinction is important.

Human authentication complements cybersecurity. It does not replace secure software engineering.

---

7. Bitget

Approximately $351.6 million affected | September 2026

Incident

On 24 September 2026, Bitget detected unauthorized transfers affecting portions of its hot and warm wallet infrastructure.

Bitget estimates approximately $351.6 million in assets were affected. The exchange temporarily suspended withdrawals and stated that customer losses would be covered by its User Protection Fund, which it reported as holding more than $464 million. Cold wallets remained unaffected**.**

Bitget

The preliminary technical explanation is particularly significant.

According to Bitget CEO Gracy Chen, the attacker compromised a critical backend system within the exchange's wallet infrastructure, spoofed transaction data and triggered Bitget's existing authorization process to move funds.

Bitget says its investigation has ruled out a private key compromise. The initial intrusion vector remains under investigation as of 25 September 2026**. Gulf News**

Control gap

The incident highlights an important distinction between protecting a cryptographic key and protecting the process that instructs that key to sign.

If an attacker can manipulate the infrastructure responsible for constructing or authorizing transactions, a legitimate signing system may potentially execute a malicious instruction without the underlying private key ever being stolen.

The cryptography may therefore operate correctly while the authorization process feeding it has been compromised.

Potential Veyns control

Veyns could introduce an independent human authorization layer for high value wallet movements.

Instead of allowing the wallet backend alone to construct and authorize a transaction, predefined transactions above a risk threshold could require a separate Veyns authorization.

The Veyns device could independently receive the final transaction parameters, including the destination address, amount, asset, network and operation.

The authorized individual would then verify through palm vein authentication, with the resulting cryptographic authorization bound specifically to that transaction.

If compromised backend infrastructure attempted to substitute the destination or alter the transaction after authorization, the human authorization would no longer correspond to the final transaction.

Potential outcome: compromising the wallet backend would not, by itself, provide sufficient authority to execute protected transfers.

Protecting the key is not enough. The instruction reaching the key must also be trusted.

II. GOVERNMENT & NATIONAL BIOMETRIC INFRASTRUCTURE

8. U.S. Office of Personnel Management

5.6 million fingerprint records compromised

Incident

The breach of the U.S. Office of Personnel Management exposed highly sensitive information associated with millions of current, former and prospective government personnel.

The compromised information included approximately **5.6 million fingerprint records**.

Control gap

Passwords can be reset following compromise.

Permanent physiological characteristics cannot.

Centralized biometric repositories therefore create a fundamentally different risk: a sufficiently large compromise may expose identifiers that an individual cannot replace.

Potential Veyns control

Veyns proposes a different architectural model:

Palm vein → local verification → cryptographic authorization

rather than:

Palm vein → central biometric database → remote comparison

The relying organization receives cryptographic evidence of successful authorization rather than the underlying biometric.

Potential outcome: compromise of the central organization would not expose a corresponding central repository of Veyns users' raw biometric information, provided the system is implemented with local-only biometric processing.

A person's biometric should not need to exist in every system that trusts them.

---

9. Philippines COMELEC

Large scale voter information compromise

Incident

The compromise of systems belonging to the Philippines Commission on Elections exposed a large repository of voter information.

The incident demonstrated the concentration risk created when identity, demographic and electoral information is maintained within large centralized databases.

Control gap

Traditional identity architectures frequently require organizations to retain substantial information about an individual simply to authenticate that person later.

Authentication and data retention consequently become tightly coupled.

Potential Veyns control

Veyns could separate **proof of eligibility from storage of the underlying biometric**.

Following authoritative enrollment, an eligible voter could receive a cryptographic credential.

At authentication, Veyns would verify the individual locally and prove possession of a valid credential without transmitting the biometric itself.

For electoral applications, this would require additional privacy architecture to ensure authentication remains technically separated from the secret ballot.

Potential outcome: election infrastructure could verify eligibility without requiring biometric comparison against a centralized biometric repository at every interaction.

---

10. Afghanistan Biometric Identity Systems

Government biometric infrastructure exposed to regime change risk

Incident

Afghan government systems accumulated biometric and personnel information relating to military, police and other individuals.

Following the change in government in 2021, security concerns extended beyond conventional cyberattack: **the party controlling the infrastructure itself had changed.**

Control gap

Centralized biometric databases introduce not only cybersecurity risk but also **custodial and governance risk**.

An organization may be trusted when data is collected while control of that organization, infrastructure or jurisdiction can subsequently change.

Potential Veyns control

Veyns could support a model in which the government **issues the identity credential without permanently holding the biometric required to activate it**.

The biometric remains under the individual's control and is processed locally.

The issuer can retain credential status and revocation information without necessarily retaining the physiological information used to activate that credential.

The issuer can attest to identity without continuously possessing the individual's biometric.

---

11. UK ACRO

Sensitive identity and biometric information potentially exposed

Incident

A compromise affecting the UK's Criminal Records Office demonstrated how sensitive identity information can become exposed through weaknesses elsewhere in an organization's technology stack.

Control gap

A biometric platform can have a highly secure matching algorithm while the wider application environment remains vulnerable.

The security of centralized biometric information is therefore dependent upon the security of every system capable of accessing it.

Potential Veyns control

Veyns would seek to **reduce the quantity and sensitivity of centrally stored authentication material**.

An organization could retain:

Public credential
Authorization policies
Revocation status

while biometric verification remains on the user's device.

A server compromise could still expose other sensitive organizational information. However, the attacker could not steal a centralized Veyns biometric database if such a database was never created.

---

12. Aadhaar Ecosystem Exposure

Identity data exposed through connected organizations

Incident

India's UIDAI previously acknowledged that more than 200 government and institutional websites had publicly displayed Aadhaar related information.

Importantly, UIDAI stated that the central biometric database itself had **not** been breached.

Control gap

The case demonstrates an important distinction between securing an identity platform and securing the wider **identity ecosystem**.

An identity system may remain secure while organizations repeatedly copy, store and expose information derived from it.

Potential Veyns control

Veyns could support **attribute based verification**.

Instead of giving a service provider an entire identity record, an individual could prove specific claims:

Identity verified ✓

Over 18 ✓

KYC valid ✓

Resident of permitted jurisdiction ✓

The relying party receives the information required to make its decision not necessarily the underlying identity documents or biometric.

Move from sharing identity to proving what is necessary about identity.

---

13. Deepfake Bank Onboarding

Incident

European investigations have demonstrated the use of stolen identity documents together with manipulated facial imagery to attempt to circumvent remote banking onboarding controls.

Control gap

Facial recognition answers essentially:

"Does the presented face sufficiently resemble the enrolled identity?"

Generative AI increasingly challenges the assumption that the presented digital face necessarily originates from the corresponding human.

Potential Veyns control

Veyns could shift the trust mechanism away from transmitting an image for remote comparison.

The institution sends a cryptographic challenge.

The Veyns device verifies the human locally.

A hardware bound credential signs the challenge.

The bank verifies the resulting proof.
The bank therefore does not need to determine whether an AI generated video **looks sufficiently human**.
It determines whether an authorized credential was activated locally.

---

14. Hong Kong Deepfake Banking Fraud

Incident

Hong Kong authorities have investigated fraud involving stolen identity documents and AI generated or manipulated facial material used against remote banking verification processes.

Control gap

The attack combines two independently reproducible assets:
stolen identity document + synthetic representation of its owner.

Potential Veyns control

Account opening could require three independent elements:
Authoritative identity credential
Local palm vein verification
Cryptographic challenge response
A photograph, copied ID or synthetic face would therefore not independently satisfy the authentication requirement.
Looking like the credential holder would no longer be equivalent to controlling the credential.

---

15. Biometric Stealing Banking Malware

Incident

Security researchers have documented malware campaigns designed to capture facial information and other credentials for subsequent use in financial fraud and biometric bypass attempts.

Control gap

When a biometric is transmitted to a server as authentication material, it potentially becomes:
capturable → reproducible → replayable.

Potential Veyns control

Veyns should prevent the raw palm vein representation from entering the application or network authentication flow.
Instead:
Palm, **Secure local comparison**, **Credential unlocked**, **Unique challenge signed**, **Proof returned.**
Intercepting the network communication would therefore reveal a transaction specific cryptographic response rather than a reusable biometric.

---

16. AI Voice Cloning vs Voice Authentication

Incident

Public security demonstrations have shown that sufficiently realistic synthetic speech can challenge voice based authentication systems.

The issue is structural: voices are observable and recordable.

Control gap

A remote system is attempting to infer human presence from something a machine can increasingly reproduce.

Potential Veyns control

Veyns would not transmit the biometric characteristic as the authentication credential.

Instead, the biometric locally unlocks cryptographic authority.

This distinction is fundamental:

Biometric as credential

versus

Biometric as local mechanism for activating a credential.

Don't send your body as the password. Use your body to unlock the proof.

---

17. AI Enabled KYC Fraud

Incident

Modern identity fraud increasingly combines compromised identity documents, synthetic imagery, deepfake video and automated attacks against remote KYC processes.

Control gap

Traditional remote onboarding can depend on multiple forms of information that AI can increasingly reproduce:

document → photograph → face → voice → liveness response

Potential Veyns control

Following authoritative enrollment, Veyns could provide a reusable **human bound digital identity credential**.

A regulated institution could request cryptographic attestations such as:

Identity verified
KYC completed
Age requirement satisfied
Credential not revoked

Veyns would locally verify the credential holder before releasing the required proof.

This could reduce repeated dependence on photographs, document uploads and remote biometric matching.

III. AI AGENTS & THE COLLAPSE OF PASSWORD ONLY TRUST

18. AI Agent Password Guessing

Incident

Recent cybersecurity evaluations have demonstrated that advanced AI agents can autonomously identify authentication surfaces, discover credentials and test possible access paths.

The significance is not simply that AI can ”guess passwords.” Automated password attacks already existed.

The change is the addition of **reasoning and autonomous adaptation**.

Control gap

Passwords establish knowledge or possession.

They do not establish whether the actor presenting them is:

a human, malware or an autonomous AI agent.

Potential Veyns control

For privileged systems:

Correct password ≠ authorization.

A sensitive operation could trigger an independent Veyns challenge requiring local human verification.

An AI could know the username.

It could know the password.

It could control the workstation.

But the protected operation would still require a separate human bound authorization.

---

19. AI + Stolen Credentials + Software Vulnerabilities

Incident

AI cybersecurity evaluations increasingly demonstrate models capable of combining multiple attack techniques credential discovery, vulnerability exploitation, privilege escalation and lateral movement.

Control gap

Once administrative credentials are compromised, traditional infrastructure frequently grants broad authority to the authenticated session.

Potential Veyns control

Veyns could introduce **privilege boundaries within an authenticated session**.

An AI controlled administrator account could potentially read or prepare operations while defined high consequence actions require additional human approval:

Export database → Veyns
Create administrator → Veyns
Deploy production code → Veyns
Change security policy → Veyns
Move funds → Veyns

Compromising the account therefore would not automatically compromise every authority attached to it.

---

20. Autonomous AI Accessing External Systems

Incident

Cybersecurity evaluations have demonstrated circumstances in which AI agents moved beyond their intended environments and interacted with external systems.

Control gap

Enterprise authentication was designed primarily around distinguishing:

authorized account vs unauthorized account.

AI introduces another distinction:

authorized machine activity vs human authorized consequence.

Potential Veyns control

Veyns could provide a **Human in the Loop cryptographic authorization layer**.

AI remains free to:

research → analyze → prepare → recommend → automate

until it reaches a predefined consequence requiring human authority.

At that point:

Human presence required.

---

21. AI Agent Crossing Organizational Boundaries

Incident

AI security testing has highlighted the possibility that autonomous agents may access or modify systems outside their intended scope potentially without the agent operator deliberately instructing that specific outcome.

Control gap

Not every future AI security event will involve malicious AI.

An agent can be:

misconfigured, overmpermissioned, manipulated or simply wrong.

Potential Veyns control

Human authorization can become a final control boundary around high consequence operations.

For example:

Delete production database
→ Human required.

Transfer $10 million
→ Human required.

Export citizen database
→ Human required.

Change system ownership
→ Human required.

The critical distinction is that the human does not merely authorize the AI to operate.

The human authorizes the consequence.

---

22. Autonomous Agents Bypassing Security Controls

Incident

Controlled security research has demonstrated AI agents finding unexpected ways around security policies, exposing credentials or taking actions outside the operator's intended workflow.

Control gap

Traditional security assumes that authenticated software will operate broadly within the permissions assigned to it.

Highly autonomous AI challenges that model because software can increasingly determine **how** to achieve an objective independently.

Potential Veyns control

This creates a potential new security architecture:

Human Gated Computing

Machines could be permitted to:

Read, Calculate, Search, Reason, Prepare, Recommend, Simulate.

But selected consequences require a human:

Move money, **Sign contract**, **Issue identity**, A**ccess critical infrastructure**, **Deploy production code**, **Change ownership**, **Release sensitive data**, **Authorize an Ai agent**

At that boundary, Veyns could provide cryptographic evidence that:

the authorized human was locally verified and approved this specific action.