

# How Do I Prove To A Corporation I Am ME?

## Make Hacking Worthless Again.

A different kind of white paper.

*An invention waiting to be built to solve a problem that is fast becoming universal.*

---

Wylie Eden

Lake Country, British Columbia, Canada

Sole Inventor · 18 Patents Filed with USPTO · 2026

*I am just a guy, an outsider to your world, who had a vision based on a life altering experience. I believe that what I have put forward here gives rise to answering a key question facing society today: how do I prove to a corporation I am ME? In a world where corporations themselves have more rights than the individuals, there has to be a better way. And I believe this is it.*

— Wylie Eden, inventor

This is not a technical brief written by a committee. It is not a pitch deck engineered to impress a room. It is an idea — one that started with a single life experience, grew into a protocol, and now sits behind eighteen filed patents. The question at the centre of it has not changed from the beginning.

The pages that follow explain what has been envisioned, how it works, and what changes if it exists. You do not need to be an engineer to follow it. That was a deliberate choice.

This paper is being released in June 2026. In the days before publication: 404 Media reported that hackers obtained access to high-profile Instagram accounts by prompting Meta's own AI support agent — no stolen credentials, no phishing campaign, just a natural language request. A nursing professional posted that Facebook permanently banned her account on the same action as her face verification — she never once accessed the account she had been asked to verify. Waves of passive users received "SOC" bans with no warning, no explanation, and no appeal path — then were offered a paid subscription as the route to recovery. These are not incidents surfaced by investigative journalism after months of digging. They appeared in public subreddits, in real time, on the same day this paper was completed. The problem has not been approaching a crisis point. It has passed one.

## Part One: What I Envisioned and Why

Think about the small town bank. The teller knows your face. Knows your voice. They do not ask for a password — they verify the person standing in front of them. That instinct never broke. What broke is that we forgot it when we moved online — and replaced biological recognition with a PIN and a security question. BIT Seal™ restores that instinct at global scale, cryptographically.

The idea started with a personal experience I will not detail here. What I can say is that I found myself unable to prove to a corporation that I was the person I had always been. I had all the right answers. None of them were accepted. And I thought: there has to be a way to make identity a mathematical fact instead of a memory test.

That experience exposed something that every person in those Reddit threads already knows, even if they have never put it in these words: in the current system, the user is merely a rental tenant — subject to arbitrary eviction from their own digital existence. Not by hackers. By the platform itself. The landlord changes the locks and asks no questions. The tenant has no deed. BIT Seal™ is the deed.

The original concept was simple. What if, at the moment you create an account — or update a current one — you leave behind something that is yours alone — not a password you invented, not a phone number that belongs to a carrier, not an email address that can be reassigned — but a cryptographic fingerprint derived directly from your biology? And what if recovering that account required presenting the same biology, live, in real time?

That is BIT Seal™. That is the core of everything that followed.

Think about the structural mismatch for a moment. The tools being used to compromise accounts today — AI-driven credential stuffing, deepfake voice synthesis, real-time phishing engines — are battering rams. The tools built to stop them — security questions, SMS codes, backup email addresses — are screen doors. The attackers have automated, scaled, and industrialized the attack. The defence has not moved. BIT Seal™ is the first response built to the same standard as the attack: cryptographic, biological, hardware-bound, and irreversible.

And the shift it proposes is profound in its simplicity. Every existing system asks: do you know the right answer? BIT Seal™ asks: are you the right person? Replacing bureaucratic permission with biological fact. Your face, your voice, your hardware — those are not answers you can forget, lose to a breach, or have reassigned to a stranger. They are you. Biological authority does not expire.

*Stop guarding the key. Become the key.*

I should say something about the name. BIT Seal™ is what I call it today. It has gone by other names — Silligumkey, among others — and it will likely carry different names in different contexts and industries as it finds its applications. The name does not matter yet. What matters is the function. And the function is broad enough, foundational enough, and applicable enough across enough industries that it will wear many names before it is done. A protocol this horizontal does not belong to one name any more than it belongs to one platform.

## FROM AN APP TO A PROTOCOL

The first version was a mobile app — a working prototype called **Hacker Smasher**, demonstrating the enrollment and recovery flow in a way anyone could follow. What I did not anticipate was how quickly the idea outgrew the app. As the technical depth increased, as the attack scenarios multiplied, as the platform implications became clear — the app became a demonstration and the protocol became the product.

The protocol is called BIT Seal™. It is the specification behind the app, the patents, and every platform integration described in this document. The app shows what it looks like. The protocol defines what it is.

*From a demo app born from frustration to a global standard of identity that makes hacking mathematically impossible to sustain.*

## THE FIVE FACTORS (2 TO N) — WHY ALL FIVE, WHY AN AND GATE

Most multi-factor authentication systems use an OR gate. You can use your password OR your phone OR your email. The implicit assumption is that a single factor is sufficient. That assumption is the vulnerability — every case study in the previous section is a proof that it is not.

BIT Seal™ uses an AND gate. All five factors are required. Not most of them. Not any combination. All five. Simultaneously. Live. This is not a UX compromise — it is the security model. The strength of the identity credential is the product of five independent verification factors (2 to N), not the weakest one.

### Face Map

A

68+ stable landmark distances and angular relationships extracted from facial geometry. Not a photo comparison — a structural measurement. Changes in lighting, aging, expression do not affect the underlying geometry.

### Voice Print

B

The resonant geometry of the vocal tract — the shape of the instrument, not the words spoken. Immune to recordings and voice synthesis because it captures the physical structure of the speaker's anatomy.

### ID Check

C

Government-issued document cross-validated against the live person presenting it. Ties the biometric credential to an external identity anchor at enrollment.

### Real-Human Audit

D

Liveness detection that rejects photos, recordings, deepfakes, and masks in real time. Confirms that a living person — not a representation — is present at the moment of verification.

### Hardware Handshake

E

Cryptographic binding to the specific enrolled device via its Secure Enclave. The identity credential is partially device-bound — which enables the triage mechanism described later in this document.

Five independent factors go in. One irreversible cryptographic hash comes out. That hash has never existed before — it is not a record of your face, not a scan of your fingerprint, not a stored voice sample. It is a mathematical object derived from the combination of all five, simultaneously, from a living person. Remove any single factor and you get a completely different output. Present a recording instead of a live person and the derivation fails. That is the invention.

The Secure Enclave is where this processing happens today — a locked chip inside your phone that no software can access. But the protocol is not the chip. The chip is the current best vessel for something that could run on any trusted execution environment.

***The innovation is the AND-gate. The innovation is the combined hash. Those are the things that have not existed before.***

## **A DESIGN FLOOR — NOT A CEILING**

---

Because the architecture is built on an AND gate, the factor count is a design parameter — not a fixed constraint. A platform integration may require two factors or five or more. The factors are modular. The AND gate is the architecture. Scaling from 2 to N independent inputs does not change the model — it strengthens it. Five is the current implementation. The floor is two. The ceiling does not exist.

## **Part Two: The Architecture**

This section is written for a general reader. The technical depth is here, but so is the plain-language explanation of what each piece does and why it exists. One thing to keep in mind throughout: the Secure Enclave is mentioned often because it is the current best environment for running this protocol securely. It is not the invention. It is the room. The invention is what happens inside it.

### **THE AND-GATE — WHY THE COMBINATION IS THE CREDENTIAL**

---

Every existing identity system treats factors as alternatives. Password OR phone number OR email. The implicit logic is: any one of these is sufficient to prove who you are. This is the vulnerability. Any one of them can be stolen, reassigned, or social-engineered. The whole stack collapses through its weakest link.

BIT Seal™ inverts this. The five factors are not alternatives — they are simultaneous requirements. All five. Live. From the same person. At the same moment. The cryptographic output is derived from their combination, not from any one of them individually. This means the credential cannot exist without all five being present. An attacker who has four of the five factors — including a stolen device — still has nothing. The identity is the product of the combination. That product has never existed as a storable, transferable object before.

### **WHERE THE PROCESSING HAPPENS — AND WHY IT STAYS THERE**

---

Every modern smartphone contains a specialized chip that operates in complete isolation from the main processor. Apple calls it the Secure Enclave. Android equivalents exist under various names. It cannot be accessed by the operating system, by applications, or by anyone with physical access to the device. It processes and stores cryptographic material that never leaves its boundary.

The five factor (2 to N) inputs arrive at this boundary. The hash derivation runs inside it. The signed credential exits. No raw biometric data ever leaves. The only output is a hash and a confirmation that the derivation succeeded. The protocol could run on any equivalent trusted execution environment — hardware security modules, future embedded chips, other device architectures. The SE is today's best vessel. The protocol is not bound to it.

Why not bound to it: the Secure Enclave is a Trusted Execution Environment — an isolated compute boundary where sensitive operations run outside the reach of the operating system, applications, and anyone with physical access. Any hardware that provides that boundary can run this protocol. A Hardware Security Module in a data centre provides the same guarantee. A future embedded chip in a credit card could provide it. A government-issued identity document with cryptographic capability could provide it. As hardware architectures evolve, the protocol travels with them — because the protocol is not the chip. It is the logic of what happens inside any chip that earns the name.

## WHAT A HASH IS — AND WHY IT CANNOT BE REVERSED

---

A cryptographic hash is a one-way function. You can put data in and get a fixed-length output. You cannot put the output in and recover the data. SHA-3, the algorithm used in BIT Seal™'s core derivation, produces a 256-bit output from any input of any size. Two inputs that differ by a single bit produce completely different outputs. There is no mathematical path from the output back to the input.

The math behind why this cannot be reversed: a 256-bit output has more possible values than there are atoms in the observable universe. To find the input that produced a given hash by brute force, you would need to perform more computational operations than there are atoms in the universe — at current processing speeds, longer than the age of the universe to complete. This is not a technical limitation waiting to be engineered around. It is a mathematical wall. SHA-3 does not get weaker as computers get faster — it was designed with that adversarial trajectory already priced in.

This means the hash stored at enrollment contains no biometric data. A server that holds your BIT Seal™ hash cannot reconstruct your face, your voice, or any factor that produced it. If the server is breached, the attacker gains a string of characters that is useless without the living person who generated it.

## ZERO STORAGE — WHY THERE IS NO DATABASE TO BREACH

---

The most common objection to any biometric system is storage. What happens when the database is breached? It is a fair question — and the people asking it are right to be afraid. Facebook settled a \$650 million biometrics lawsuit. Clearview AI scraped three billion faces without consent. Every centralized biometric database ever built has either been breached, subpoenaed, or sold. The fear is not paranoia. It is pattern recognition.

**BIT Seal™ was designed in direct response to that fear. The answer here is: nothing happens when the database is breached. Because there is no database.**

BIT Seal™'s security model is architecturally opposite to every existing identity system. Existing systems store identity data centrally. BIT Seal™ stores a non-reversible hash in two places only: on the enrolled device and in an encrypted cloud backup. Both require all five live verification factors to access. There is no central biometric database. There is no record of your face, voice, or any factor. There is a hash. And the hash is worthless without you.

There is no location data. No IP history. No device fingerprint log. No behavioral profile. No session metadata retained after the POOF Protocol closes. Zero storage is not a privacy feature added on top of the system. It is the system. The protocol was designed from the first principle that any data retained is a liability — to the user and to the platform holding it. The only thing that exists after an enrollment event is a hash that cannot be reversed, cannot identify you without your biology, and cannot be stolen in any form that is useful to an attacker.

This matters legally as well as technically. GDPR Article 17 — the right to erasure — requires platforms to delete personal data on request. BIT Seal™ satisfies that requirement by design, not by process. There is no biometric record to delete. Destroying the per-factor helper data cryptographically eliminates any possibility of re-deriving the hash — permanently, verifiably, without relying on a deletion workflow to work correctly. Erasure is a mathematical event, not an administrative one.

*We store nothing. Not because it is convenient. Because we designed a system where storing it was never necessary.*

## THE POOF PROTOCOL — EPHEMERAL SESSIONS, NO RESIDUE

The zero-persistence model has a name: the POOF Protocol. During a recovery event, the raw biometric inputs exist in volatile RAM only — never written to disk, never transmitted, never persisted. The moment verification succeeds and the Sovereign Token is issued, the session closes. All biometric material is gone. There is nothing to intercept later because there is nothing left.

Two mechanisms enforce this. The first is manual: once the user confirms account restoration, a scrub command overwrites all session-related data across nodes. The second is automatic: if the user forgets, a 24-hour time-to-live purges all session data automatically. This is distinct from the 24-month re-enrollment cycle — that is about biometric freshness. This is about the recovery session itself. A captured session is useless after 24 hours, and there is no server holding anything before that. The session cannot be replayed because it was never stored.

*We provide the bridge, then we burn the bridge — so no one else can cross it. Utility, not a database.*

## Part Three: The World This Makes Possible

BIT Seal™ is not a product for one platform or one industry. The protocol is horizontal. What follows is a sketch of what changes in four sectors if this exists.

### SOCIAL PLATFORMS

Facebook has three billion monthly active users. Industry estimates place account compromise at one to five percent annually — between thirty and one hundred and fifty million accounts that need recovery every year. Meta spends approximately five billion dollars per year on safety and security. The support chains that handle failed recoveries absorb a significant portion of that headcount. They fail the majority of complex cases.

Recovery is currently a pure cost centre for every platform. It only costs them money — in support headcount, in infrastructure, in reputational damage when the recovery fails and the story goes viral. BIT Seal™ changes that equation. The real owner verifies biometrically. The account suspends. The contact list is alerted. Access is restored. No agent. No form. No loop. A successful recovery event generates a fee. The biggest cost centre in trust and safety becomes a revenue line. That is the CFO argument for integration — not altruism, not regulation, not brand pressure. A direct conversion from loss to income.

The integration model is deliberately frictionless. Platforms are not asked to rebuild their security infrastructure. They are asked to whitelist one token — a cryptographically signed Sovereign Token issued by BIT Seal™ after successful five-factor verification. That token serves as an absolute override to all other recovery methods: email, SMS, 2FA, security questions. The platform adds one acceptance path. Everything else stays exactly as it was. The Override Protocol requires no architectural change to the platform's existing systems — other than automatic acceptance of the Sovereign Token.

Every unrecovered account is also a live weapon against the platform. A hacked account repurposed for spam, crypto-scams, or manipulation — what might be called a zombie account — costs the platform far more than the original recovery would have. Every zombie account erodes user trust, triggers regulatory scrutiny, and saturates the platform's own abuse detection with noise. BIT Seal™ does not just recover accounts. It eliminates the zombie account population by making recovery possible in the first place.

The trend inside major platforms is moving in exactly the wrong direction. Faced with an identity problem they cannot solve, platforms are collecting more — not less. Location data. IP history. Device fingerprints. Behavioral signals. Session metadata across apps and services. The logic is triangulation: if we cannot verify who you are directly, we will build a dense enough profile that we can infer it. Meta now explicitly informs users that even if they disable location services, the platform will estimate their location from their IP address. The screen reads: "How we'll use this information — to help keep your account secure." Location tracking sold as a security feature. The data collection is the product. The security framing is the justification.

This approach fails on its own terms. Behavioral profiles can be learned. IP addresses can be spoofed. Device fingerprints can be cloned. Location history can be replicated. Every signal that can be observed can eventually be faked — and the attacker only needs to fake it once, while the legitimate user has to match it consistently. The more complex the behavioral model, the more ways a legitimate user can accidentally fail it — travel, VPN, new device, network change. The platform ends up with a surveillance apparatus that locks out real users and can still be defeated by a determined attacker.

BIT Seal™ collects none of it. No location. No IP log. No behavioral profile. No session history. The architectural direction is the opposite: instead of building a larger inference engine to approximate identity, verify it directly and discard everything else. One enrollment event. One hash. No residue. The user is not a profile to be matched against. They are a biological fact to be verified.

There is a second-order consequence worth naming. When platforms make mass automated banning decisions with no human review and no appeal path, users do not conclude the system made a mistake. They conclude the system is working against them. That distrust is a brand damage event — and the users most damaged are the longest-tenured, most loyal ones. A 16-year user who loses their account with zero evidence and an immediate automated rejection does not come back. [1] BIT Seal™ enrollment creates an audit trail. The platform issued a cryptographic confirmation of identity at enrollment — not just at that first moment, but refreshed with every re-verification and every 24-month re-enrollment cycle. That record cannot be erased by the same AI that issued the ban. Which means the platform can no longer say it had no way to verify who the account belonged to — it verified them at enrollment, and that verification is on record.



That audit trail has regulatory teeth. If government agencies or class action litigants examine a pattern of mass automated bans, the central question becomes: did the platform have a verified identity on record for these users at the time of the ban decision? Without BIT Seal™, the answer is no — and the platform's liability exposure is diffuse. With BIT Seal™ enrollment records in place, the answer is yes — and a ban executed without human review against a verified enrolled user is a materially different legal event. Enrollment does not just protect users. It creates the evidentiary foundation for claw-back.

## **THE PROOF OF NEED: FACEBOOK'S FAILED ATTEMPT AT THE SAME SOLUTION**

The most compelling evidence that this protocol is needed is not found in the failure cases. It is found in what Facebook has already tried to build.

A parent recently posted that her son had been subjected to months of account restrictions for no stated reason. During that period, Facebook required him to submit selfie videos every few weeks as proof of being human. He also submitted a government-issued ID. Facebook rejected both. After months of this, his account was permanently disabled.

His solution — described in the post as a "glimmer of hope" — was to create a new account with a different name on the same computer, same internet connection, same device. It passed immediately.

Read that sequence carefully. Facebook's identity verification system rejected a real person presenting a selfie video and a government ID — then accepted an unnamed fake account on identical hardware. The system is not broken. It is doing exactly what it was built to do. The problem is what it was built to do. A selfie video with no cryptographic enrollment record is a liveness check that is not anchored to any specific person. It is a test for "human" — not a test for "the human who owns this account." A government ID rejected without a biometric match is just a document. Neither one, alone or together, constitutes an identity proof without the enrollment event that preceded them.

***Facebook is already asking users to present biometrics. It just does not know what to do with them. The architecture is missing. That is the gap BIT Seal™ fills.***

In BIT Seal™, the government ID check (Factor C) is one of five factors combined at a single enrollment moment into an irreversible hash. Every subsequent verification is measured against that hash. A new account with a different name on the same device cannot produce the same hash — because it cannot present the same face, voice, liveness confirmation, ID, and hardware signature that produced the original. The fake account that slipped through Facebook's check would not survive enrollment. The real person who was rejected would recover in seconds.

**This is not a hypothetical gap. It is a demonstrated one. The world's largest social platform, with billions in security spending, is already reaching toward biometric signals — selfie videos, government IDs — with no underlying architecture to make them mean anything. They have identified the symptom. This document prescribes the cure — and eighteen filed patents back every line of it. The gap between what they reached for and what they built is exactly the gap BIT Seal™ fills. [2]**

## THE MARKETPLACE GATE — THE RIGHT INSTINCT, THE WRONG ARCHITECTURE

---

In June 2026, a Reddit user posted to r/facebook: "I've been waiting for my reason to leave Facebook, and I just found it." After a handful of sales on Marketplace, Facebook presented a gate: "We've detected unusual activity on your account. Before you can publish this listing, confirm your identity." The user refused to submit their government ID. They deleted Facebook.

Read that reaction carefully. The gate is correct. Requiring identity confirmation before a financial transaction is exactly the right instinct. The backlash is not against the concept of identity verification. It is against Facebook being the custodian of the credential. Handing a government ID to a platform that settled a \$650M biometrics lawsuit, that shut down its own face-recognition system under regulatory pressure, and that users have stopped trusting — that is the friction. The gate requires trust in the gatekeeper. That trust is gone.

BIT Seal™ changes the equation. The user presents their biology. A non-reversible hash is generated on their device. Facebook never receives the ID. Facebook never holds the biometric. The gate operates — the transaction is authorized — without Facebook becoming the custodian of the credential that authorized it. The user who would never hand Facebook their passport would consent to a verification that Facebook cannot store, cannot breach, and cannot monetize. The gate is right. The architecture is missing.

## FINANCIAL INSTITUTIONS

---

Dark web monitoring services currently serve financial institutions — banks and credit unions are alerted when customer credentials surface on criminal markets. That intelligence goes to the bank. It does not go to the platform, and it does not yet have a response layer that makes the detected credential worthless before it is used. BIT Seal™ provides that layer. A stolen credential set is useless if account access requires live biometric re-verification from the enrolled holder. [3]

## CREDIT BUREAUS

---

The credit bureau model is structurally broken. SSN plus knowledge questions equals identity — and that equation is trivially defeated by anyone with access to the dark web markets where SSNs trade for cents. [4] IP-12 replaces the SSN-as-identity model with a biometric hash at the point of bureau account creation and at every subsequent access event. Bureau access — including freeze and unfreeze — requires live biometric verification from the enrolled account holder. A phone call to a support agent cannot bypass this gate. [5] The bureau never holds a copy of the identity credential — only a hash reference. The enrolled person's biology is the gate.

Equifax has already reached the same conclusion. Their Kount 360 platform now includes document verification and facial recognition through a partnership with Incode — applied to lenders and businesses doing identity proofing on their customers. The biometric layer exists. It is just positioned to protect the bureau's clients rather than the person whose file it actually is. The architecture is validated. The gap is in who it protects. IP-12 closes that gap by placing the biometric gate at the consumer layer — so that the person whose identity is at stake is the one who holds the key.

## AI AGENTS AND AUTONOMOUS SYSTEMS

As AI agents gain the ability to take consequential actions on behalf of users — sending money, executing contracts, managing accounts — the authorization layer becomes critical. IP-18 establishes biometric pre-authorization as the gate before any high-consequence agent action. The agent acts when the human has verified. Not before. This is the architecture that makes human-in-the-loop a technical reality rather than a policy aspiration.

**On June 1, 2026, 404 Media reported that hackers obtained access to high-profile Instagram accounts by prompting Meta AI directly. No stolen credentials. No phishing. No technical exploit. A request. The AI, deployed as a support agent, complied. This is the predictable outcome of deploying AI agents without a biometric authorization gate. A prompt is not a verification. IP-18 is the gate that makes the difference.**

---

[1] Addendum B — "Sixteen years, zero evidence, immediate rejection." Facebook account disabled mid-conversation, no warning, no violation. Meta Verified support described as "less than worthless." All legal channels slower than the automated system.

[2] Addendum B — "Facebook's failed biometric verification." Platform required selfie video and government ID over months — rejected both. A fake account on identical hardware passed the same check immediately.

[3] Addendum B — "Bank drained in 50 minutes." iCloud compromised, phone factory reset, \$5,000 drained via Cash App, Apple Pay, and Zelle. Wells Fargo confirmed transactions via the email channel the attacker controlled.

[4] Addendum B — "SSN-squatted bureau accounts." An 18-year-old discovered their SSN already associated with an unknown phone and email at Experian and TransUnion — before they had ever opened a credit account.

[5] Addendum B — "Credit freeze bypassed by a phone call." Attacker called TransUnion and Experian and bypassed both phone verification layers. Victim told: "There is nothing stopping the thief from coming in and unfreezing your credit again."

## Part Four: The Evidence Is Already Everywhere

People sometimes ask who would want a product like this. The honest answer: if they do not already know they need it, they soon will. The accounts below are not cautionary tales about careless people. They are previews. They are what happens to careful people when the system built to protect them fails — and it will fail, because it was never built on a solid foundation. How do you put a value on irrefutable proof that you are you? You cannot. You can only measure what it costs when that proof does not exist.

Reddit alone is inundated with these stories. Scroll any day of the week across r/Outlook, r/facebook, r/IdentityTheft, r/personalfinance, r/CRedit — and you will find hundreds of posts from real people who have lost accounts, credit files, financial records, photos, businesses. The platforms differ. The mechanism differs. The outcome is always the same. These are not edge cases surfacing occasionally. This is a constant, rolling tide across every field where identity touches a corporation — which is every field.

**The Identity Theft Resource Center documented 353 million breach victims in 2023. Two years later, the FTC reported Americans lost \$2.1 billion to social media scams in 2025 alone — eight times the 2020 figure. In January 2026, a single unencrypted database was discovered containing 149 million stolen passwords — 48 million Gmail accounts, 17 million Facebook — harvested by AI-powered infostealer malware running at machine scale. The FBI puts total US internet crime losses at \$20.9 billion for 2025, with \$893 million attributed directly to AI-enabled attacks: voice cloning, deepfakes, synthetic identities. The trajectory is not a trend. It is an acceleration — and AI did not cause it. AI industrialized it.**

***Not isolated incidents. A real-time feed of a problem that does not pause — until now.***

Ten documented cases are collected in Addendum B. They span Microsoft Outlook, Facebook, Instagram, credit bureaus, and financial institutions — gathered from public posts on Reddit between 2025 and 2026. They were chosen not because they are extreme but because they are typical. They appear in real-time feeds on r/Outlook, r/facebook, r/IdentityTheft, r/personalfinance, and r/CRedit on any given day. Each one follows the same structure. Each one ends the same way. Thousands more could have been sourced — but we all know the problem. The ten below are simply proof that we do.

## **THE COMMON THREAD**

Every one of these cases follows the same structure. A real person exists. A corporation holds something that belongs to them — an account, a photo, a credit file, a financial record. The corporation requires proof of identity before granting access. The proof required is a possession: a password, a phone number, an email address, a PIN. Call it security trivia — a knowledge test designed for an era before industrialised credential theft. The possession was compromised, transferred, or lost. The real person — the one whose face and voice and fingerprints have not changed — has no way to assert that fact.

What follows is always the same sequence. The attacker changes the password. Changes the recovery email. Switches the 2FA to a number they control. The platform's own security tools — designed to protect the account — are turned against the real owner in sequence. Each hardening step the attacker takes makes the real owner less visible to the system. The hacker's phone number becomes the Source of Truth. The real owner ceases to exist as far as the platform is concerned — a digital eviction executed not by bypassing the security model but by weaponizing it. The fortification that was supposed to protect them is the instrument of their removal.

The conventional response — change your password, add 2FA, revoke sessions — fails for a structural reason: every one of those actions passes through the same credential layer the attacker already controls. The user is fighting from inside a burning building using tools the attacker handed them. The platform cannot distinguish the real owner from the attacker because both are operating through the same account. There is no exit from that loop inside the account. The real owner needs a door the attacker cannot reach.

## **THE OUT-OF-BAND KILL SWITCH**

BIT Seal™ provides that door. Biometric self-suspension is an out-of-band signal — it does not pass through the account at all. The enrolled owner fires a biometrically-signed suspension instruction directly to the platform. The instruction is signed by the only credential that matters: the hardware-bound, biometrically-derived enrollment key that was established at account creation. The platform receives a cryptographically valid command from the biological owner and is obligated to honour it — suspending all active sessions immediately, regardless of what credentials the attacker currently controls.

The attacker cannot countermand it. Generating a valid suspension countermand requires the enrolled biometrics. The attacker never enrolled. Their session — however deeply embedded, however many security settings they have changed — dies the moment the real owner fires the signal. The account belongs to whoever can produce the enrollment hash. The attacker cannot produce it. The owner can. That asymmetry is absolute.

This is not a stronger password. It is a different class of action entirely — one that exists outside the account's own authentication layer, cannot be blocked by someone who has captured that layer, and resolves in seconds rather than support queues. The platform's tools were turned against the owner. The owner's biology turns them back.

The corporation, unable to verify identity directly, defaults to the only tool it has: policy. Policy rejects. The loop closes. The real person is on the outside — ghost in the machine of their own account.

This is not a failure of effort. Corporations spend billions on security. It is a structural failure. The credential was never the identity. It was always just a key. And keys can be copied, reassigned, replaced — and turned against you by the platform designed to help you. Biology cannot.

---

## Close

**Think of it as identity notarization. A notary confirms who you are once. That confirmation is trusted everywhere — not because the notary is always present, but because the act of confirmation is on record. BIT Seal™ does the same thing cryptographically. At enrollment, your biology is notarized into a mathematical object that no one can fake, forge, steal, or replicate. The identity claim never becomes someone else's. It does not require the platform to be acting in good faith. It does not depend on a phone number that can be reassigned or an email address that can be compromised. The credential refreshes every 24 months — mandatory re-enrollment ensures it represents who you are today — but the claim of ownership never transfers. Biology enforces that.**

The mission is simple: to restore digital lives through physical truth. Every case in this document is a version of the same failure. Every one of them has the same solution.

At sufficient scale, this protocol does not just protect individual accounts. It makes the underlying attack economically unsustainable. A stolen credential — however complete — is worthless if account access requires live biometric re-verification from an enrolled person. There is no attack pathway that does not require the attacker to be biologically present. Hacking does not disappear. It becomes impossible to sustain at the scale and economics on which it currently operates.

I did not put this forward because I saw a market. I designed it because I experienced a failure and could not find anyone who had solved it. Every case in this document is a version of that failure. Every one of them has the same solution. That might be the most important thing in this document.

*If the system does not recognize the creator, the creator must build a system that the original system cannot refuse.*

The answer is not a better password. It is not a faster support form. It is not a smarter policy. It is a mathematical fact — derived from biology, stored on hardware, verified in real time, and impossible to transfer.

**Identity is not a possession. It never was. It is time the infrastructure caught up to that fact.**

---

Wylie Eden

Lake Country, British Columbia, Canada

Sole Inventor · 18 Patents Filed with USPTO

[linkedin.com/in/wylie-eden-289785401](https://www.linkedin.com/in/wylie-eden-289785401)

2026 · All rights reserved

## Addendum A: The Filed Innovations

Eighteen patents have been filed with the United States Patent and Trademark Office. What follows is a plain-language description of the core innovations — what each one covers and what problem it solves.

**IP-01      The Combined Biometric Hash**

Five or more independent verification factors — biometric, documentary, procedural, and hardware — combined into a single non-reversible cryptographic credential via HKDF derivation inside the Secure Enclave. The five-factor model is the security floor — the AND-gate architecture scales to N factors. The foundational patent covering the AND-gate identity model.

**IP-02      Dual-Layer Secure Storage**

Primary storage in the device Secure Enclave, encrypted cloud backup as redundancy. Both require live biometric re-verification. Neither contains raw biometric data.

**IP-03      Biometric Account Self-Suspension**

The enrolled identity asserts control and freezes the account — regardless of what credentials an attacker has already changed. Triggered by the real owner's biometric assertion, not a support form.

**IP-04      Social Graph Alert Broadcast**

Upon self-suspension, the account's contact list receives an automated alert that the account has been compromised and the real owner is recovering it. Neutralizes the attacker's most valuable asset — trusted relationships — before they can be monetized.

**IP-11      Credit Card Biometric Gate**

Biometric authorization at the point of card issuance and card activation. A new card cannot be activated without live biometric re-enrollment from the account holder.

**IP-12      Credit Bureau Biometric Interrupt**

A biometric pre-authorization gate at the point of a credit inquiry. Bureau access — including freeze and unfreeze — requires live biometric verification from the enrolled account holder. A phone call to a support agent cannot bypass this gate.

**IP-16      Hardware Attestation Path**

Eliminates the fuzzy extractor variance problem by binding the identity derivation to hardware attestation via the Secure Enclave. The device itself participates in the cryptographic proof, removing the requirement for probabilistic biometric matching tolerances.

**IP-17      Rolling Hash Re-enrollment**

Biometric credentials are refreshed on a 24-month cycle, enforcing biometric freshness and ensuring the stored credential represents the current enrolled person. Mandatory re-enrollment is a security feature, not an inconvenience.

**IP-18      Human Authorization Gate for AI Agents**

Biometric pre-authorization required before an AI agent or automated system can execute high-consequence actions on behalf of a user. The agent acts — but the human must verify first.

A further nine innovations cover cross-platform recovery orchestration, partner API permission models, device-bound enrollment connectors, and additional application-layer protocols. Total filed: 18.

## Addendum B: Documented Case Studies

The following cases were gathered from public posts on Reddit between 2025 and 2026, across r/Outlook, r/facebook, r/IdentityTheft, r/personalfinance, and r/CRedit. They are presented without editorial modification. Each one was selected not because it is exceptional but because it is representative — a version of this case appears in the same thread, in the same subreddit, on any given day of the week.

### THE LAST PHOTO OF A MOTHER — LOCKED BEHIND A BROKEN PASSWORD

A Reddit user posted that they have been locked out of their Outlook account for twelve years. The account holds the last photo of their mother, who died in 2014. They have the correct password. But 2FA is tied to a phone number reassigned years ago, and the backup email is also inaccessible. Recovery forms have been submitted repeatedly. No resolution. The photo remains inside a system that will not let the real owner in.

### WATCHING AN ATTACKER TAKE EVERYTHING — IN REAL TIME

Another user watched their Outlook account get hacked while they were still logged in. The attacker changed the password, changed the recovery email, changed the 2FA — replacing every possession factor in sequence. The real owner had nothing left the platform would accept. Standard recovery failed. The account belonged to someone else within minutes.

### TWO MINUTES TO PERMANENTLY DISABLED — TWELVE YEARS GONE

A Facebook and Instagram user received three emails in sequence: 12:58 AM — account suspended, 180 days to appeal. 12:59 AM — Instagram email confirmation code (attacker adding their email to the connected account). 1:00 AM — review unsuccessful, account permanently disabled. The 180-day appeal window lasted two minutes. The review was automated. Facebook's own data export system could not generate a download link. Twelve years of data, inaccessible to everyone.

### CREDIT FREEZE BYPASSED BY A PHONE CALL

An identity theft victim had frozen their credit at all four bureaus with secret PINs. An attacker called TransUnion and Experian and talked their way through phone verification — bypassing both. Credit unfrozen. Hard inquiries appearing for new accounts. The victim was told: "There is nothing stopping the thief from coming in and unfreezing your credit again." The PIN is pointless. The security question is pointless. A human voice is all it took.



### **EXACT INFORMATION. TEN YEARS. STILL DENIED.**

A Reddit user was locked out of their Outlook account after suspicious activity appeared. They responded correctly — logged in and changed the backup email immediately. Then came the account recovery form. They completed it with exact information. Denied. They tried again. Denied again. They escalated to a human at Microsoft support and provided additional account information directly. Still denied. The account is over ten years old. Inside it: active job applications, important correspondence they cannot afford to miss. The recovery form does not assess whether the information is accurate. It assesses whether the information matches what it currently expects — and after suspicious activity alters account state, what the form expects and what the real owner knows can diverge. The real owner has the exact information. The form has a different definition of exact. His closing words: "I am so pissed off with Microsoft — their customer support is non existent and I have no idea how to get into my account of 10+ years." That is not a technical complaint. That is what the absence of a solution sounds like from the other side. BIT Seal™ does not ask what the form expects. It asks who the person is.

### **THE ORPHANED ACCOUNT — NO ATTACKER, NO THEFT, NO WAY BACK**

A parent created an Outlook account for their young son. The password was lost before the account was ever properly used. No attacker. No compromise. Just a credential gone before the account had a history. The recovery workflow failed. Support provided no path. The parent's own suggestion: "With all the AI we have, they could do better asking relevant questions that only I can answer." That instinct points directly at the problem — knowledge-based questions can be social-engineered, guessed from data breaches, or simply never established when an account has no history. BIT Seal™ does not ask questions. It verifies biology.

### **ONE YEAR LATER — PERMANENTLY DISABLED, ASKING ABOUT WORKAROUNDS**

A Facebook user's account was permanently disabled after they were hacked and the hacker's posts were reported. The automated system penalized the victim — the account associated with the offending content — not the attacker who posted it. One year on, there is no appeal path, no resolution, no human to contact. The user is not asking how to recover the account. They have given up on that. They are asking whether enough time has elapsed to create a new one. The closing note: "I only really want Messenger back. Facebook is all just adverts anyway." What was taken was not a profile — it was a phone.

### **ONE HACK, THREE ACCOUNTS — AND A RECOVERY FORM THAT REJECTS THE TRUTH**

An Outlook account was hacked. The attacker changed the email and password. That single compromise cascaded immediately: the Xbox account linked to that Outlook address was lost with it. The PlayStation account followed — the recovery email was now the compromised Outlook address, and every recovery form rejection led nowhere. The form was not malfunctioning. It was working exactly as designed — it asked for the current credentials, and the current credentials are whatever the attacker set them to. The real owner knows what the account used to contain. The form accepts only what it contains now. Those are two different answers, and only one of them passes.

### **"IN ONE SWIPE META DESTROYED MY ABILITY TO CONNECT WITH FAMILY AND FRIENDS"**

An 80-year-old user's Facebook account was gone. Not hacked by a sophisticated attacker. Not caught in a credential breach. Gone — permanently banned, no explanation, no appeal path. For an 80-year-old, Facebook is not a social network. It is the infrastructure through which they stay connected to family. One automated decision severed that infrastructure without warning, without recourse, and without any mechanism for the real person to assert that they are real. BIT Seal™: biometric enrollment creates a verifiable identity anchor that exists independently of the platform's account infrastructure. The enrolled person can assert their identity even after the account is disabled — the biological proof predates the ban decision.

### **SIXTEEN YEARS, ZERO EVIDENCE, IMMEDIATE REJECTION — AND A MASSIVE CLUB**

A Facebook user lost a sixteen-year-old account with no warning, no explanation, and no evidence of any violation. The notification arrived mid-conversation with a friend. Just: gone. They paid for Meta Verified support — described as "less than worthless." The appeal was rejected immediately. They then documented every available legal channel: State Attorney General, FTC, LegalShield, Small Claims Court in the Northern District of California. All slower than Meta's automated system. Their summary of the comment thread: "Welcome to the Club. It's a MASSIVE Club and it's growing daily." The scale of that club — visible in any Facebook-related subreddit on any given day — is the market signal. Every person in it is a person the existing system has no answer for. BIT Seal™ does.

### **THE PLATFORM AS THE THREAT — AI MASS-BANNING AS A BUSINESS MODEL**

Observers in the same thread raised a theory that has gained traction: Facebook's AI is not making mistakes. It is deliberately disabling accounts at scale to force migration to a paid subscription model. Whether the intent is deliberate or incidental, the structural reality is the same — an automated system is making permanent identity decisions at a scale no human review process can keep up with, and the appeal layer is the same automated system that issued the ban. This represents a new and distinct threat class: the platform itself as an adversarial actor against its own users. Every prior failure mode in this document assumed the platform was at least nominally trying to help the real owner recover access. This one does not. BIT Seal™'s biometric anchor matters here precisely because it exists independently of the platform's intent. A verifiable enrollment record cannot be erased by the same system that disabled the account. The real owner's claim is cryptographic — it does not require the platform to be acting in good faith to be valid.

### **"IT'S THEIR FAULT — AND I'M SUPPOSED TO PAY?"**

A Reddit user was simultaneously banned from Facebook and deactivated from Instagram on May 25, 2026 — both actions triggered by Meta's automated systems on the same day. The stated reason: "SOC." The user had been a passive member for over six years — posting rarely, following approximately ten pages, uploading two or three landscape photos. No content violations. No warnings. The Instagram account was recovered. The Facebook account was not. The appeal failed immediately. The "Facebook/hacked" recovery feature was blocked after a single use — the system flagged it as abuse for being used too quickly. The data download page returns a blank screen. Six years of personal history: inaccessible to everyone. Meta then offered a path forward: Meta Verified, a paid subscription service. The user's response: "It's THEIR fault, and I AM supposed to pay?" This is the platform monetizing the damage caused by its own automated systems — converting a support failure into a revenue event. They called it a Sword of Damocles: the permanent, arbitrary threat hanging over every user regardless of conduct. The platform has become, in their words, "the metastasis of the internet." BIT Seal™ enrollment means the biological owner of an account retains a verifiable claim that exists independently of any platform decision — including the decision to charge for recovery from a ban the platform itself caused.

### **"CONFIRM YOUR IDENTITY" — THE GATE WITH NO ARCHITECTURE BEHIND IT**

A Reddit user posted to r/facebook in June 2026: "I've been waiting for my reason to leave Facebook, and I just found it." After making several sales on Facebook Marketplace, they were shown a gate: "We've detected unusual activity on your account. Before you can publish this listing, confirm your identity to help us make sure it's really you." The gate required submission of a government ID. The user refused and deleted Facebook. Their comment: "No thanks. It was the only reason I had FB anymore, so good reason to delete it." The gate is the right instinct. The backlash is not against identity verification — it is against Facebook holding the credential. A government ID submitted to a platform that settled a \$650M biometrics lawsuit and shut down its own face-recognition system under regulatory pressure is not a verification. It is a liability transfer. BIT Seal™ removes Facebook from the custody chain entirely. The biology is verified. The hash is generated on the device. Facebook authorizes the transaction without ever holding what authorized it.

### **"THEY JUST ASKED." — META AI AND THE INSTAGRAM TAKEOVER**

On June 1, 2026, 404 Media reported that hackers had successfully obtained access to high-profile Instagram accounts by prompting Meta AI. The AI, deployed as a technical support agent, was manipulated into granting account access — no stolen credentials, no phishing campaign, no sophisticated technical exploit. A natural language request was sufficient. The report described it as "the extreme risk of offloading technical support to AI." This is not a failure of the AI model's intelligence. It is a failure of authorization architecture. An AI agent acting without biometric pre-authorization from the enrolled account holder is an attack surface, not a security layer. IP-18 requires that before any AI agent executes a consequential action on a user's account, the enrolled identity asserts biological authority first. The agent acts when the human has verified. Not before. A prompt is not a verification. Biology is.

### **FACE VERIFIED. ACCOUNT CREATED. PERMANENTLY BANNED. SAME DAY.**

A nursing professional posted to r/facebookdisabledme: "I don't care for Facebook and never have. But for nursing jobs it has great opportunities to build connections. Yes I have LinkedIn, Facebook was just a supplemental. Here's the issue: I didn't even get to access my effing account! I made the account and same spot did my face verification for no reason because they permanently banned me." The platform asked for a biometric — a face scan — and then banned the account on the same action. This is the architecture failure in a single sentence. Facebook's face verification is unanchored. It establishes that a human is present. It does not establish which human, because there is no enrollment record linking the biometric to the account identity. The scan was accepted and discarded in the same moment. It proved nothing because there was nothing to prove it against. BIT Seal™ inverts this: the biometric is not a one-time gate. It is the enrollment anchor. Every subsequent verification — at login, at recovery, at any high-consequence action — is checked against the same hash generated at the moment of account creation. The biology that opened the account is the same biology required to access it. Facebook verified a face. BIT Seal™ verifies the owner.

### **LOGGED IN. LOCKED OUT. THE ATTACKER HAS FULL CONTROL.**

A user posted to r/cybersecurity\_help: "Hacker stole my Microsoft account but forgot to change the password, and I logged in but they still have full control." The real owner is authenticated — actively logged in — but every action that would restore control routes a verification code to the attacker's email. Change the recovery email? Code goes to the attacker. Change the password? Code goes to the attacker. Set up new 2FA? Code goes to the attacker. The platform's own security system is now working for the attacker, not the owner. Being logged in means nothing when the recovery infrastructure has been reassigned. This case has no AI involvement, no sophisticated exploit, no deepfake. Just a password and a changed recovery email — and every security gate on the account now routes through whoever controls that address. The enrolled biometric anchor is the only thing that changes this. If recovering or modifying the account's security infrastructure requires the live biology of the person who created it, the attacker's email address is irrelevant. They cannot present the face, the voice, and the hardware that enrolled the account. The recovery chain cannot be seized because it is not a possession. It is a biological fact.

### **"SOMEONE ONLY NEEDED MY NAME AND PHONE NUMBER TO ACCESS MY ACCOUNTS" — BMO, 40 YEARS**

A user posted to r/PersonalFinanceCanada: their Google account was hacked over the weekend and a charge appeared on their BMO MasterCard. They called BMO. BMO asked only for their name and phone number — no address, no account verification, no identity check of any kind. The user hung up, convinced they had reached a scam number. They called back. Same result. BMO only sent a verification code when the user specifically asked for one. The user's summary: "My fear is that someone only needed my name and phone number to access my accounts." They are considering leaving BMO after forty years. A commenter noted: "Wild to me that they haven't dropped voice verification considering how easy it is to duplicate now with AI." The commenter is correct — and the problem is broader than voice. Name is public record. Phone numbers are leaked in every data breach. Voice can be cloned in minutes with freely available AI tools. Each of these factors is a single possession or a single recording. BIT Seal™'s five-factor simultaneous AND gate cannot be defeated by any one of them — or all of them — because the gate requires five live factors at the same moment from the same person. A cloned voice fails the face check. A stolen phone fails the voice check. Stolen data fails the hardware attestation. The AND gate is not a stronger password. It is a different class of proof entirely.

*These are not edge cases. These are the logical outcomes of a system where identity is a possession — and possessions can be taken, lost, never established, surrendered to an automated system that cannot tell the owner from the attacker — or deliberately revoked by a platform with no obligation to reverse course.*

## Addendum C: Technical Appendix

This appendix is provided for readers with a security engineering or cryptography background. It summarises the enrollment and verification protocol, the key derivation chain, and the relationship to existing authentication standards.

### ENROLLMENT PROTOCOL — STEP BY STEP

---

1. The user initiates enrollment on their registered device. All biometric capture occurs inside the device's Secure Enclave (SE) or equivalent Trusted Execution Environment (TEE). Raw biometric data never leaves this boundary.
2. Five factor inputs are captured simultaneously: face geometry, voice print, government ID confirmation, real-human audit signal, and hardware attestation token. Simultaneous capture is a protocol requirement — sequential capture is rejected.
3. Each factor is reduced to a fixed-length byte representation inside the SE. These five byte arrays are concatenated with a device-bound salt and passed to the HKDF extract phase.
4. HKDF (RFC 5869, HMAC-SHA-3) produces a pseudorandom key (PRK) from the combined input. The expand phase derives the final 256-bit enrollment hash from the PRK.
5. The enrollment hash is stored in two locations: device-bound in the SE (primary), and in an encrypted cloud backup (secondary). Both require all five live factors to access. No raw biometric data is stored in either location.
6. A hardware-signed credential is issued confirming enrollment. The signing key is device-bound and non-exportable.

### VERIFICATION PROTOCOL

---

At any verification event — login, recovery, or high-consequence action — the device re-derives the hash from a fresh live capture of all five factors. The derived hash is compared to the stored enrollment hash inside the SE. A match issues a Sovereign Token scoped to the session. No hash or biometric material leaves the device during this comparison. The session is ephemeral: all biometric material in volatile RAM is purged on session close (POOF Protocol). A 24-hour TTL enforces automatic purge if the session is abandoned.

### KEY DERIVATION — WHY HKDF OVER FUZZY EXTRACTION

---

Fuzzy extractors are the conventional approach to biometric key derivation. They tolerate measurement variance by encoding error-correction data alongside the derived key. The tradeoff: the helper data leaks partial information about the biometric input, and variance tolerances create attack surface — an adversary who can supply inputs within the tolerance boundary may succeed.

BIT Seal™ uses HKDF with hardware attestation (IP-16) to eliminate this tradeoff. The hardware attestation factor provides a cryptographically stable anchor — device-bound, non-replayable, and not subject to biological variance. Biometric variance in the other four factors is normalised before the HKDF extract phase rather than tolerated after it. The result: a deterministic derivation with no helper data and no variance-based attack surface. This is the specific technical contribution of IP-16.

## **RELATIONSHIP TO FIDO2 / WEBAUTHN**

---

FIDO2 and WebAuthn authenticate the device via a public/private key pair. The private key is device-bound. A biometric gesture may unlock the key locally — but the biometric is not key material. It is a local access control step. The credential that authenticates to the server is the device key, not the biology.

The architectural consequence: FIDO2 authenticates possession. If the device is compromised or cloned at the OS level, the private key is accessible without the biometric. BIT Seal™ authenticates biology. The enrollment hash cannot be derived without the living person present — the device is a necessary component but not a sufficient one. A stolen device produces nothing.

BIT Seal™ is additive to FIDO2, not competitive. A platform using FIDO2 for standard authentication can layer BIT Seal™ verification for high-consequence actions — account recovery, security infrastructure changes, financial authorisations — where device possession alone is insufficient proof of identity.