CLEAR

WHITEPAPER

Identity Redefined: *The Necessity of a Multi-Layered Approach*

Table of Contents

INTRODUCTION

Identity: The Foundation of Digital Trust

In today's digital landscape, identity is the critical infrastructure that enables or blocks every high-value interaction, from accessing sensitive information to completing transactions to building lasting relationships. Despite identity's central importance, our collective understanding of what identity is and how it's defined remains anchored in outdated practices. We've been conditioned to equate "identity" with a document or credential, when true identity is inherently multidimensional and dynamic. This thinking creates vulnerabilities that traditional approaches cannot address.

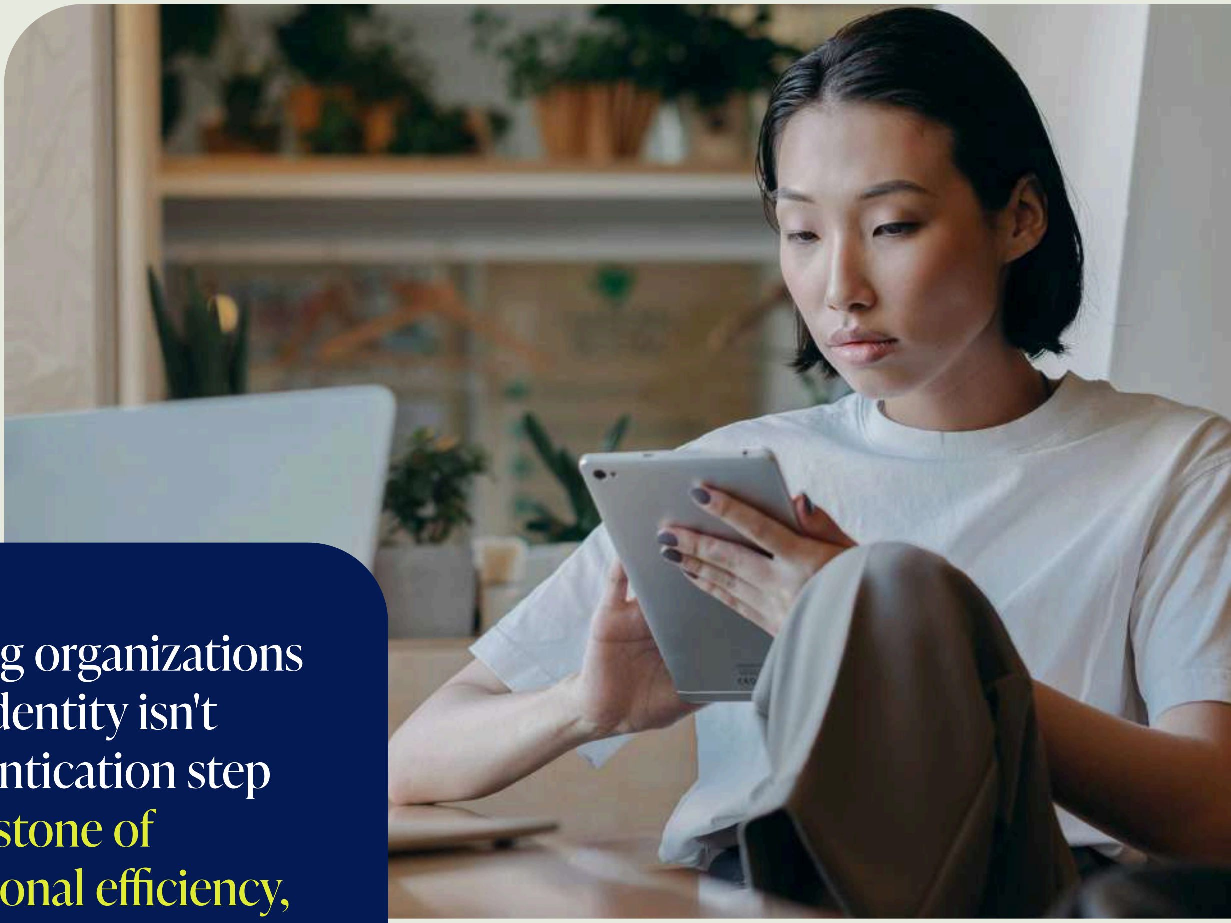
The result is a cascade of operational challenges that impact every sector of the economy:

1. **Healthcare providers** struggle with manual and fragmented digital processes that delay care and compromise data security.
2. **Workforce security teams** face social engineering attacks that exploit traditional multi-factor authentication (MFA) weaknesses.
3. **Financial institutions** balance battling fraud and chargebacks with maintaining smooth customer experiences.
4. **Hospitality brands** strive to deliver direct-to-door experiences that increase loyalty without sacrificing security.
5. **Rental companies** fight fraud that threatens assets and operational efficiency.

The issue is foundational. We've built systems focused on what we have (such as credentials, devices, and IDs) rather than who we are (the person behind the device). This approach worked in simpler online environments, but AI-powered threats and digital-first operations have permanently altered the identity landscape.

Today's environment demands a multi-layered solution that confirms identity at every critical touchpoint. When strategically implemented, this approach strengthens protection while eliminating unnecessary friction, demonstrating that security and experience are complementary priorities.

INTRODUCTION



Forward-thinking organizations recognize that identity isn't merely an authentication step — it's the cornerstone of security, operational efficiency, and customer experience.

In this whitepaper, you'll learn:

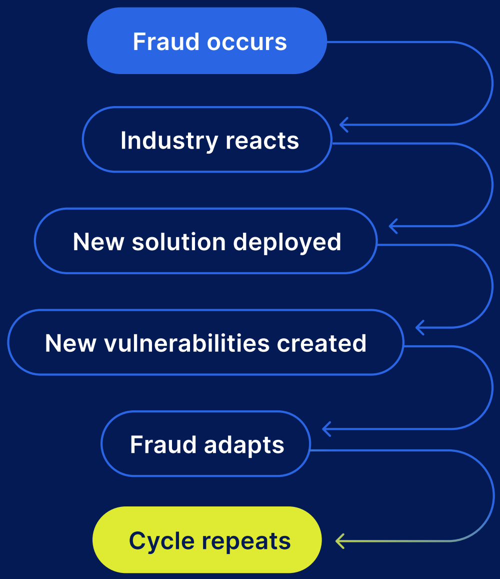
- ✓ Why identity forms the foundation of digital security and how traditional methods leave businesses exposed to sophisticated threats
- ✓ How a multi-layered identity approach provides the highest level of identity assurance — preventing fraud, minimizing risk, and protecting sensitive data
- ✓ How our collective understanding of identity has been shaped by historical limitations
- ✓ How leaders in healthcare, real estate, and telecommunications configured different identity check combinations to meet their unique security and compliance needs

INTRODUCTION

The Evolution of Identity: From Documents to Digital Assurance

Identity is the set of characteristics that define a person and distinguish them from others. Yet our understanding has been reduced to documents — not because this approach is most secure, but because institutions historically needed tangible forms of verification.

This document-centric approach created a fundamental problem: Identity systems have been developed reactively, in response to fraud that already occurred rather than anticipating emerging threats. The result is a perpetual security gap where fraudsters consistently stay one step ahead of protective measures. Each new identity system fixes yesterday's vulnerabilities while inadvertently creating openings for tomorrow's attacks.



Fraud occurs

Industry reacts

New solution deployed

New vulnerabilities created

Fraud adapts

Cycle repeats

A Timeline: Identity Through History

The following timeline traces how historical events have repeatedly redefined our concept of identity, showing the shift from administrative identification to security verification to today's multi-layered identity assurance.

How to read this timeline:

🟥 Red events indicate reactive responses that redefined identity after a need or crisis.

🟦 Blue events represent proactive innovations that expanded our understanding of what identity means.

1930s–1980s:

THE PAPERWORK ERA

Identity as paperwork: During this period, identity primarily serves administrative functions. Society views “identity” as simply possessing the correct document.

1936

SSNs introduced

- Responding to the Great Depression’s need for systematic benefits tracking, Social Security numbers (SSNs) are created solely for earnings histories, not intended as security credentials or identity verification.[1]
- Society’s understanding of identity becomes tied to a number rather than just physical characteristics or documentation, creating the first widespread numeric identifier.

1980s

MRZs on travel documents introduced

- Machine-readable zones (MRZs) on passports standardize identity information for border control.[2]
- Identity information becomes machine-processable, beginning the transition from human-verified identity to technologically-verified identity.

1990s–2000s:

THE SECURITY TRANSFORMATION

Identity as protection: Following security crises, society reconceptualizes identity as a security mechanism. The concepts of “identity theft” and “identity fraud” enter public consciousness.

1998

First e-passport introduced

- Malaysia introduces the world’s first electronic passport with an embedded chip storing biometric data.[3]
- Identity documentation evolves from purely physical to include hidden digital components, introducing the concept that accurate identity verification requires multiple layers.

2001

9/11 Commission expands requirements for verifying identities

- In response to the 9/11 attacks, which exposed how terrorists obtained valid identification by exploiting system gaps, identity verification transforms from an administrative convenience to a critical national security priority.[4]
- **Immediate response:** 2001’s USA PATRIOT Act expands requirements for financial institutions to verify customer identities, establishing the foundation for modern Know Your Customer (KYC) practices.[5]

2005

REAL ID Act established

- Reacting to 9/11's security failures, Congress passes the REAL ID Act to establish minimum security standards for state-issued driver's licenses and ID cards.[6]
- Identity documents become standardized across jurisdictions, establishing the concept that identity verification requires consistent, minimum security standards.

2006

U.S. introduces e-passports

- Following international pressure for enhanced border security post-9/11, the United States begins issuing e-passports with embedded RFID chips containing digital versions of the passport information and a biometric identifier (a digital photograph).[7]
- Identity verification begins to incorporate multiple layers (physical document + digital verification), establishing that stronger identity assurance requires verification across different mediums.

2010s:

THE DIGITAL EXPANSION

Identity as digital identifiers: The ubiquity of smartphones expands our understanding of identity to include biometrics, device fingerprints, and behavioral patterns.

2010

CLEAR launches the secure identity company

- CLEAR debuts in airports, enabling travelers to move seamlessly through security with biometric authentication — making experiences both safer and easier than traditional document-based methods.
- Early deployment proves consumer trust in CLEAR's approach, demonstrating that people value secure, frictionless experiences over outdated methods.

2011

Risk-based security emerges with TSA PreCheck

- The Transportation Security Administration (TSA) launches TSA PreCheck, a risk-based program that focuses security resources on higher-risk travelers by pre-screening and identifying trusted individuals.[8]
- Identity verification becomes contextual and efficient, enabling pre-vetted, low-risk travelers to experience expedited, less intrusive screening.

2013

Consumer biometric authentication introduced

- Apple introduces Touch ID on the iPhone 5S, bringing fingerprint-based biometric authentication into the mainstream consumer experience.[9]
- Consumer identity verification moves beyond “what you have” and “what you know” to include “what you are,” expanding our understanding of identity to include inherent biological characteristics.

2017

NIST Digital Identity Guidelines established

- The National Institute of Standards and Technology (NIST) publishes Digital Identity Guidelines (SP 800-63-3), establishing formal guidance on identity assurance levels (IAL) and authentication assurance levels (AAL).[10]
- Identity verification becomes recognized as contextual and risk-based rather than binary. Different scenarios require different levels of identity assurance.

Facial recognition goes mainstream

- Apple introduces Face ID with the iPhone X, bringing 3D facial recognition technology to consumer devices.[11]
- Advanced biometrics normalize the idea that your face is your identity, further cementing the concept that “who you are” physically is more definitive than “what you possess” or “what you know.”

2018–2024

Era of massive identity breaches

- A cascade of catastrophic data breaches forces industry-wide recognition that traditional security approaches have failed, exposing the personal data of hundreds of millions:
  - **SolarWinds (2020):** A supply chain attack impacts over 18,000 customers — including U.S. federal agencies and Fortune 500 companies — through a months-long espionage campaign attributed to a Russian state-sponsored threat actor.[12]
  - **MGM Resorts (2023):** A social engineering cyber attack targeting hospitality operations shuts down casino systems for 10 days, costing the company $100 million.[13]
  - **Change Healthcare (2024):** The largest healthcare data breach in U.S. history affects approximately 190 million individuals' protected health information through a BlackCat/ALPHV ransomware attack.[14]
  - The exploitation of personal data undermines traditional knowledge-based verification, forcing recognition that “secret information” can no longer be considered definitive proof of identity.

2021

MDLs introduced

- States begin adopting mobile driver’s licenses (mDLs) as digital complements to physical IDs, with Arizona, Utah, and others leading implementation.[15]
- Identity verification evolves to include selective disclosure capabilities, introducing the concept that identity is contextual — different transactions should reveal only relevant identity attributes. Technologies like MDLs make this possible. For example, they allow someone to verify they’re over 21 without revealing their full birthdate or home address.

2022

Digital identity ecosystems expand

- CLEAR1 launches, expanding beyond travel into healthcare, financial services, and other industries — proving that secure identity should follow you anywhere life takes you.
- Identity transforms from fragmented, context-specific processes to one unified solution that works seamlessly across multiple touchpoints and environments.

2023+

AI-powered identity threats increase

- As AI-powered deepfakes and synthetic identities proliferate at an unprecedented scale, organizations scramble to address threats that render traditional verification methods obsolete.[16]
- Single-factor identity verification becomes fundamentally unreliable, forcing recognition that true identity assurance requires corroboration across multiple dimensions and signals.

2023

CLEAR leads the paradigm shift

- CLEAR launches NextGen Identity+, the highest-fidelity digital identity that unlocks physical and digital experiences for members in the airport and beyond, delivering a more predictable, friction-free experience while providing enhanced security.
- Identity verification evolves from single-signal decisions to multi-signal analysis, establishing that true identity assurance requires orchestrating multiple verification methods before determining pass/fail outcomes.

Present:

THE MULTI-DIMENSIONAL REALITY

Identity as a complex ecosystem: Today, we recognize that identity is inherently multi-dimensional — not a single document or credential but a complex web of attributes, behaviors, and corroborating evidence that must be verified across multiple layers to establish genuine trust.

INTRODUCTION

2025

1 CLEAR1 sets the new standard in identity by launching its B2B platform

- CLEAR1's comprehensive identity stack approach incorporates multiple verification layers:
  - Something you have (physical ID, mobile device)
  - Your unique features (biometrics)
  - Contextual signals (location, device, behavior patterns)
  - Source corroboration (verification against trusted databases)
- The selfie (biometrics) gets matched to the portrait on the government ID, while information on the document (such as name, address, and DOB) gets verified against issuing and authoritative databases through source corroboration.
- Identity is becoming understood as a complex orchestration of multiple signals rather than a single credential or attribute, fundamentally redefining what constitutes sufficient identity verification.

Breaking the Reactive Cycle

Organizations need multi-layered identity solutions that address how identity works, not just the latest threats.

Vulnerable by Design: The Risks of Traditional Identity Verification

As identity has moved beyond documents and single identifiers, threats have evolved alongside it. The pattern is consistent and costly: Each new attack forces reactive adaptations, leaving organizations perpetually vulnerable. Organizations need to start reinforcing their approach.

Single-Layered Vulnerabilities Create Concentrated Risk

Traditional identity solutions create measurable security gaps that advanced threat actors aggressively exploit. Document-only approaches concentrate risk by creating singular points of failure that can be systematically targeted. Generative AI has made document counterfeiting cheaper and more accessible than ever, enabling criminals to create convincing forgeries. These systems lack awareness of suspicious patterns or behavioral anomalies, while technological advances continue to outpace traditional verification methods.

These limitations reflect an outdated understanding of identity as primarily document-based — a framework that has reached its limits as technology advances and threats evolve.

Modern threat actors deploy advanced multi-vector attacks.

Just as our understanding of identity has expanded over time, so has the complexity of threats enterprises face across industries. To understand why single-layered identity systems fail against modern threats, let’s examine how today's attackers orchestrate sophisticated campaigns that simultaneously exploit technological vulnerabilities, artificial intelligence capabilities, and human psychology.

Credential-Stuffing Operations

What began as simple, brute-force attacks has evolved into automated credential-stuffing operations employing stolen username-password combinations to gain unauthorized access to user accounts. Today's operations involve:

1. **Botnet orchestration:** Weaponizes thousands of devices to launch attacks at scale, overwhelming traditional defenses and creating a distributed threat impossible to contain with IP blocking.
2. **Proxy rotation:** Renders IP-based security obsolete by rotating through thousands of addresses, ensuring attacks appear to come from legitimate users worldwide.
3. **Configuration fingerprinting:** Creates tailored attack profiles specific to your security architecture, exploiting exact configurations of your environment rather than generic approaches.
4. **Intelligent retry logic:** Ensures attacks continue even after initial failures, learning from security responses to methodically overcome defenses over time.
5. **Credential validation farms:** Combine automation with human operators to defeat CAPTCHA and behavioral analytics, rendering traditional "human vs. bot" detection ineffective.

The scale of these attacks delivers significant pressure on business operations. A single credential-stuffing attack can involve millions of login attempts across thousands of websites. Success rates of 0.2–2% may seem minimal, but can translate to hundreds of thousands of breached accounts.[17] The FBI has identified synthetic identity fraud as the fastest-growing financial crime in the U.S.[18]

Roku

Credential-Stuffing Attacks[19]

In March and April 2024, streaming provider Roku suffered two massive credential-stuffing attacks that compromised

591,000 customer accounts.

Roku had a single-layered password authentication that proved insufficient against this coordinated attack, forcing it to implement two-factor authentication for all accounts afterward.

The AI Attack Vector

Artificial intelligence (AI) has rapidly accelerated the capabilities of fraudsters, proving traditional identity verification inadequate. Today's sophisticated actors deploy:

1. **Deepfakes capable of bypassing facial recognition:** Advanced neural networks now generate photorealistic facial animations that can defeat standard liveness detection, enabling unauthorized access to systems relying solely on basic biometric checks without multi-signal verification.

2. **Voice synthesis that defeats voice authentication:** Modern AI voice cloning requires just seconds of audio to create convincing replicas of executive voices, rendering single-factor voice authentication vulnerable to social engineering attacks against your organization's most sensitive systems.

3. **AI-driven forgery detection evasion:** Machine learning systems now automatically identify and counteract the specific signals your document verification systems use to detect fraud, creating perfect forgeries tailored to your organization's detection capabilities.

4. **Synthetic identity composition:** Algorithms blend stolen legitimate data with fabricated elements to create "Frankenstein identities" that pass traditional KYC validation by containing enough verifiable real-world data to trigger false acceptances in conventional systems.

Ferrari
WhatsApp Call[20]

In July 2024, Ferrari narrowly avoided a deepfake scam when fraudsters used voice-cloned phone calls to impersonate CEO Benedetto Vigna, attempting to convince an executive to assist with a fake acquisition. Despite perfectly mimicking Vigna's distinctive accent, the caller exhibited slight tonal inconsistencies that raised suspicion. The executive thwarted the attack by asking a personal verification question — the title of a book Vigna had recently recommended, which the impersonator couldn't answer.

These technologies have democratized advanced fraud capabilities, allowing even unsophisticated actors to bypass traditional identity systems with alarming effectiveness.

The Human Attack Vector

Technical vulnerabilities represent only part of the challenge. Modern identity threats increasingly exploit human psychology, weaponizing trust and authority against organizations through coordinated social engineering attacks.

Social engineering campaigns typically exploit four key psychological vulnerabilities:

1. **Authority exploitation:** Attackers pose as executives or IT managers to pressure employees into breaking security rules. When someone claiming to be a CEO calls into a support center and demands immediate access, most employees comply without questioning the request.

2. **Manufactured urgency:** Scammers create fake deadlines that force quick decisions, such as demanding that an employee approve a resource purchase (e.g., like a tablet or laptop) for a high-ranking executive who's demanding immediate access. They target employees during busy periods like quarter-end or product launches, when people are already stressed and more likely to skip security steps.

3. **Fear-based manipulation:** Criminals exploit what keeps your organization awake at night — missed compliance deadlines, competitive threats, or regulatory penalties. They know which departments fear specific consequences and craft attacks accordingly.

3. **Impersonation of trusted entities:** After studying your company, attackers perfectly copy your email signatures, security alert formats, and vendor communications. Their fake requests look identical to legitimate ones, even fooling security-aware employees.

EncryptHub

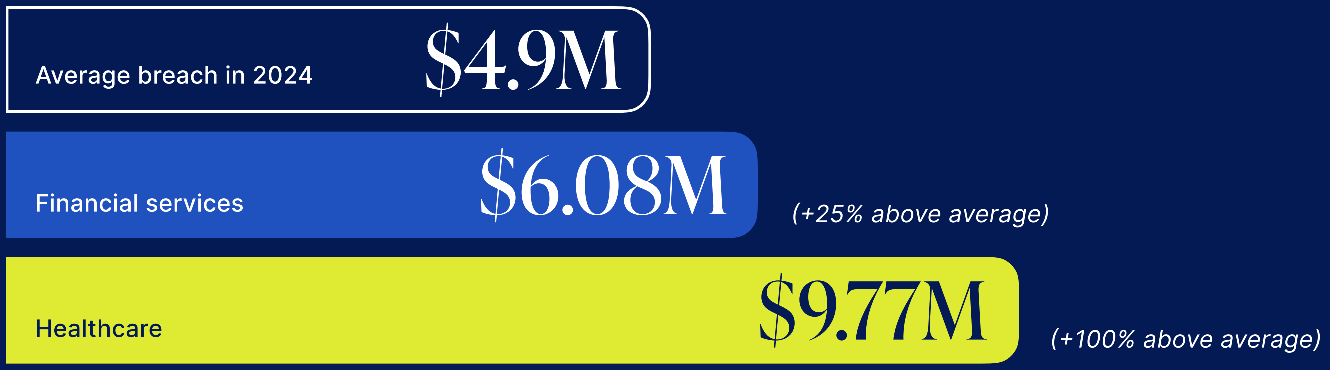
Multi-Channel Social Engineering Campaign[21]

In 2024, the financially-motivated threat actor EncryptHub demonstrated the evolution of social engineering tactics. Their approach combined multiple vectors: They made voice calls to employees impersonating IT help desk staff, created convincing phishing sites mimicking company VPNs, and targeted employees through Microsoft Teams with malicious links designed to steal Microsoft 365 credentials. This coordinated approach bypassed single-factor authentication systems by simultaneously manipulating human psychology through multiple trusted channels.

System intrusion, social engineering, and basic web application attacks represent **92% of breaches.**[22] This human vulnerability highlights why a multi-dimensional approach to identity is essential — it must protect against both technological and psychological attack vectors.

The Economic Impact of Identity Vulnerability

The cost of inadequate identity systems[23]



These elevated costs reflect market realities: Medical records and financial credentials command premium prices on dark markets, making organizations that hold this data particularly attractive targets. The higher the value of stolen data, the more persistent and sophisticated the attacks become.

Google & Facebook

BEC Attack[24]

Between 2013 and 2015, technology giants Google and Facebook fell victim to an elaborate business email compromise (BEC) scheme orchestrated by Evaldas Rimasauskas. By creating fake invoices and impersonating a legitimate Asian manufacturer that regularly did business with both companies, the attacker successfully stole $100 million. This landmark case demonstrated that even the most technologically advanced companies with substantial security resources are vulnerable to identity-based attacks, with enormous financial consequences.

These escalating costs underscore the urgency of addressing identity vulnerabilities with more robust solutions.

The Multi-Layered Solution

By connecting identity verification across multiple dimensions — what you have, what you know, who you are, and cross-checking them against each other and other authoritative sources — organizations can finally establish the level of trust required in today's digital ecosystem.

How Multi-Layered Identity Delivers Unmatched Assurance

What is a Multi-Layered Approach to Identity?

A multi-layered identity approach fundamentally reimagines how we verify who someone is. Instead of relying on isolated credentials and traditional device-based MFAs that can create single points of failure, a multi-layered identity approach weaves together multiple verification methods and signals into a comprehensive identity framework. Each layer addresses different aspects of identity, creating overlapping security that enhances protection while streamlining legitimate user experiences.

Traditional identity checks use one or two signals that can be stolen or faked. CLEAR1 uses *multiple signals* that work together and adapt, making identity fraud exponentially harder.

How Multi-Layered Identity Works

Rather than checking a small number of isolated signals, CLEAR1 draws on hundreds of signals simultaneously — from biometrics and document validation to device risk assessment and source corroboration.

Each verification layer addresses a different aspect of identity:

Confirms physical presence with advanced liveness detection and matches facial biometrics to the portrait on the government-issued ID

Scans and validates government-issued ID against fonts, marks, holograms, and tamper evidence

Validates identity details and phone ownership against authoritative and issuing sources

Proves current device possession and analyzes device signals

Screens against OFAC, PEP, sanctions, and media lists

Creates a secure, portable identity that can be reused across interactions

Customizable Security That Scales

Organizations can select which verification layers to deploy based on their specific security requirements, risk tolerance, and user experience goals.

This flexibility transforms how different industries approach their specific identity challenges. Rather than forcing a one-size-fits-all solution, multi-layered identity adapts to sector-specific needs.

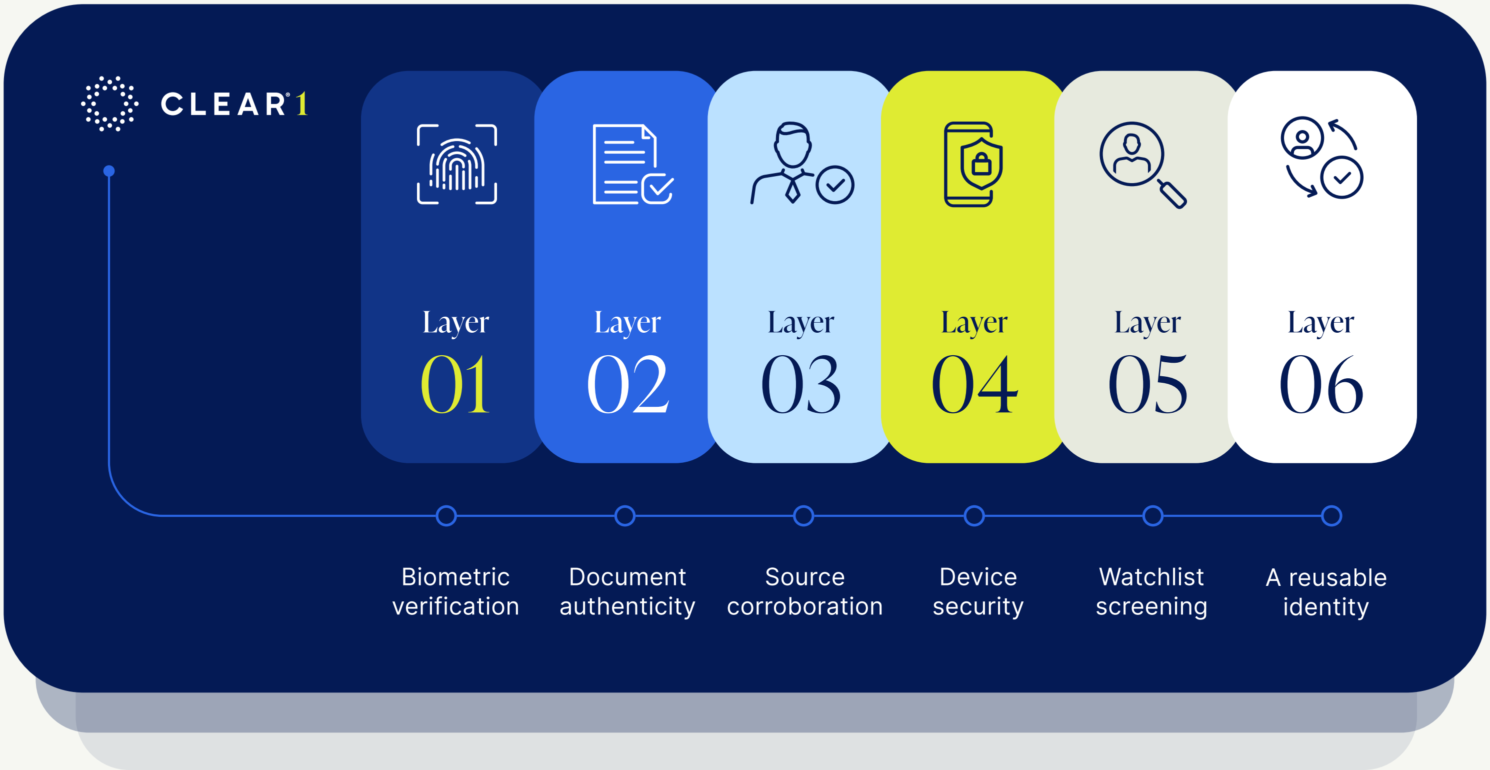
1. **Healthcare providers** might implement IAL2 (Identity Assurance Level 2) — the NIST-defined standard for remote identity verification — through liveness detection and biometric matching to ensure maximum protection for sensitive patient data while maintaining HIPAA compliance.
2. **Workforce security teams** might combine biometric matching with device analysis to prevent social engineering attacks that exploit traditional MFA weaknesses.
3. **Financial institutions** could deploy layers to meet KYC compliance by collecting key identifiers like SSNs — enabling high-assurance identity proofing that streamlines onboarding and satisfies regulatory requirements.
4. **Hospitality brands** might prioritize seamless guest experiences using streamlined verification methods with the snap of a selfie to enable frictionless direct-to-door experiences that build loyalty.

This approach creates overlapping security where each layer reinforces the others, delivering stronger protection and smoother user experiences than traditional single-factor methods.

The Anatomy of Identity Assurance: CLEAR1's Strategic Layers

While the flexibility to customize verification layers is powerful, understanding how these layers work together reveals the true strength of multi-layered identity. CLEAR1 combines several distinct verification dimensions that depend on each other to deliver comprehensive identity assurance.

CLEAR1 evaluates each identity input — including biometric data, government-issued ID, phone number, and self-attested details — and cross-checks them with each other and trusted sources. For example, a selfie is only meaningful when matched against a verified government ID; an ID is only useful if it's authentic. Each layer both stands on its own and amplifies the efficacy of the others.



CLEAR1

- Layer 01 — Biometric verification
- Layer 02 — Document authenticity
- Layer 03 — Source corroboration
- Layer 04 — Device security
- Layer 05 — Watchlist screening
- Layer 06 — A reusable identity

Layer 01

Biometric verification

***Prevents:** identity spoofing and AI-powered impersonation attempts*

CLEAR1 uses PAD-2 certified technology to confirm that the selfie being presented belongs to a live, physically present person rather than a digital representation — and it then matches the selfie to the portrait on the user's government-issued ID.

One selfie, maximum security
From a single selfie, CLEAR1 verifies liveness, confirms the biometric match to the ID photo, and blocks spoofing — all behind the scenes, with minimal friction.

Key components:

- Detects advanced spoofing attempts, such as deepfakes and presentation attacks
- Blocks technical exploits like virtual webcam injections and replay attacks
- Protects against both obvious and sophisticated forms of identity fraud

Layer 02

Document authenticity

Prevents: *credential forgery and manipulation*

CLEAR1 examines security features and formatting details of government-issued identification to detect forgeries, alterations, or counterfeit credentials.

Key components:

- Validates holograms, microprinting, ultraviolet features, and other anti-counterfeiting elements
- Confirms layouts, fonts, and proportions match official specifications
- Identifies inconsistencies that indicate tampering (e.g., signs of an original document vs. a picture of a picture/screen)
- Looks for repeating faces, signatures, or backgrounds to detect fake documents
- Validates machine-readable zones and barcodes against visible data
- Confirms the ongoing validity of documents
- Checks for non-original documents (e.g., photo of a screen)

Layer 03

Source corroboration

Prevents: *synthetic identities and sophisticated impersonation*

CLEAR1 verifies personal information against both issuing authorities and trusted authoritative third-party data sources. This dual corroboration substantiates that the information provided is consistent, legitimate, and not artificially constructed or stolen.

Key components:

- Cross-checks information on the government ID against the issuing authority, such as AAMVA and state DMVs
- Validates that the address on the ID aligns with third-party data sources tied to the same last name
- Confirms phone number ownership with telecommunications providers
- Matches the last name on the government ID to the SSN in authoritative databases

Layer 04

Device security

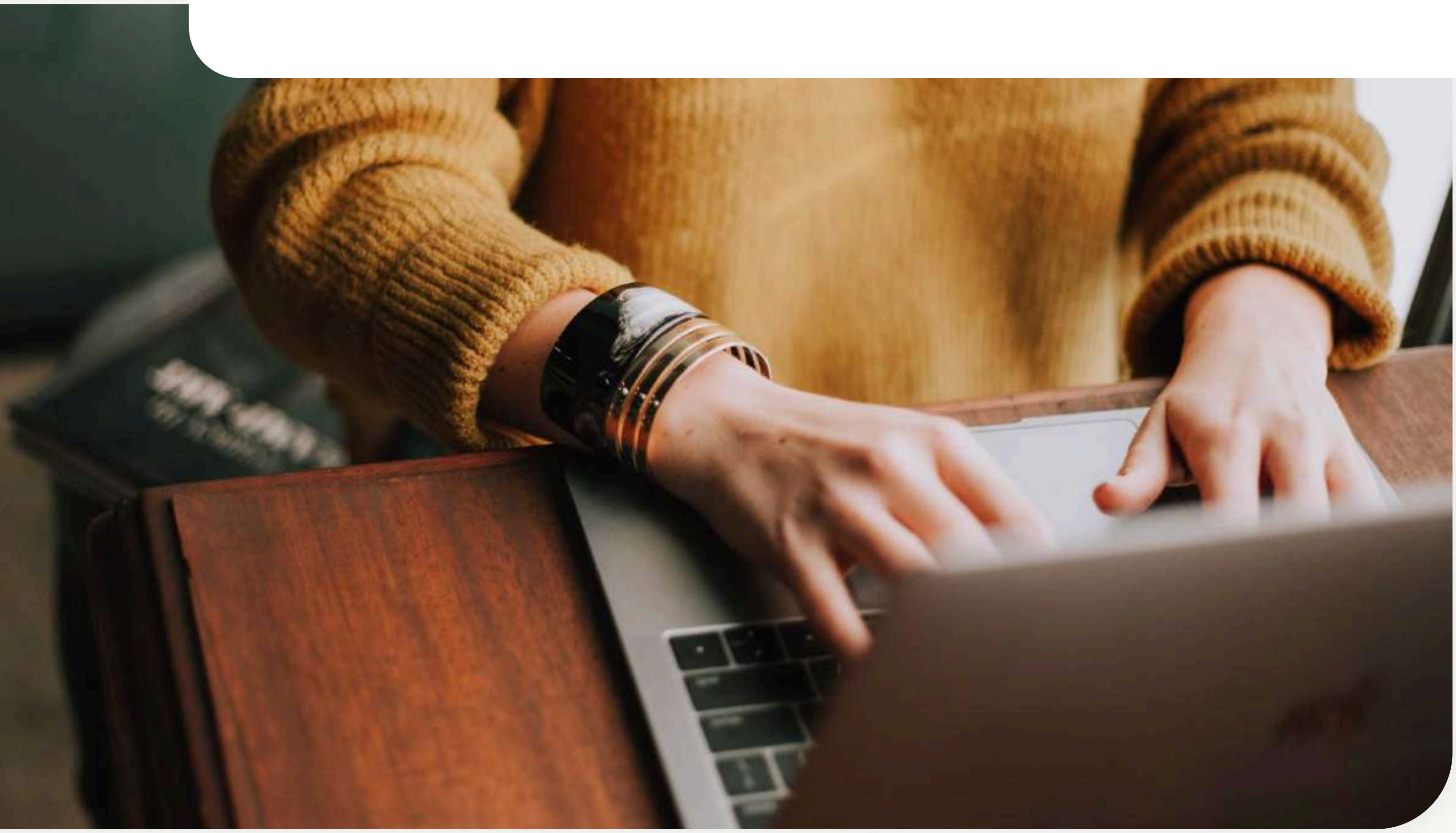
Prevents: *account takeovers through compromised device detection*

CLEAR1 evaluates 300+ device security signals across device characteristics and user behavior — including device reputation, IP address behavior, login velocity, geolocation consistency, and more — to identify suspicious patterns while allowing legitimate users to pass through smoothly.

Verified device possession
CLEAR1 confirms current device possession by delivering a one-time passcode (OTP) and verifying that the recipient matches the verified identity.

Key components:

- Detects account takeovers, credential stuffing, and synthetic identity attacks through a unified risk assessment
- Identifies bots, malware, and remote access attacks through behavioral analytics
- Assesses geolocation risks contextually without penalizing normal access patterns



Layer 05

Watchlist screening

***Prevents:** high-risk transactions with prohibited parties*

CLEAR1 broadens identity assessment beyond basic validation with optional compliance-focused screening. These checks support KYC, AML, and other regulatory requirements by identifying individuals linked to sanctions, criminal activity, or regulatory red flags.

Key components:

- Screens against OFAC and international sanctions lists
- Identifies politically exposed persons (PEPs)
- Searches for negative media associations
- Matches against industry-specific watchlists an databases

Layer 06

A reusable identity

At the center of these protective layers is the verified digital identity — a secure, portable identity object that can be reused across interactions. After a quick one-time setup, users can re-verify instantly with just a selfie, within your organization or anywhere CLEAR1 is used.

Key components:

- Functions across multiple use cases within your business ecosystem, including:
  - Account creation & onboarding
  - Biometric MFA for access to sensitive data
  - Secure password reset & account recovery
  - Authentication & check-in processes
- Helps you avoid complex regulatory changes:
  - CLEAR1 collects personal data directly from users, not your organization
  - Identity data is only shared with explicit user consent

CLEAR1

CLEAR1 transforms identity from a repetitive friction point into a business enabler, allowing organizations to establish ongoing trust without unnecessary verification steps while reducing regulatory complexity and liability.

How These Layers Connect

These verification layers don’t operate in isolation. They’re designed as an integrated verification framework where multiple signals are processed simultaneously and cross-validated against each other.

Layer 01

Layer 02

Layer 03

Layer 04

Layer 05

Layer 06

1 Biometric + Document:

The selfie from **Layer 1** gets matched against the portrait on the government ID from **Layer 2**.

2 Document + Source:

Document validation from **Layer 2** provides the personal information (name, address, DOB) that **Layer 3** checks against issuing and authoritative databases.

3 Source + Device:

Device ownership is confirmed in **Layer 4** by cross-referencing carrier records and behavioral signals with verified identity data from **Layer 3**.

4 All Layers → Reusable Identity:

Layers 1–5 feed into **Layer 6’s** reusable identity, creating a comprehensive identity profile that eliminates repetitive verification and maintains security.

Why CLEAR’s Multi-Layered Approach Works

The true power of CLEAR’s multi-layered identity solution lies not in a single component but in how these layers unite to create a comprehensive strategy that provides the highest level of assurance available today.

Here's how this strategic advantage plays out across four key dimensions:

Strategic redundancy stops attacks

Even if attackers bypass one verification method, other layers maintain protection. When someone presents a high-quality counterfeit ID (attempting to bypass **Layer 2)**, **Layer 3** immediately detects discrepancies by checking against authoritative databases. This eliminates single points of failure that criminals exploit.

Comprehensive coverage closes security gaps

Each layer addresses different attack vectors — device fraud, document forgery, and synthetic identities. Together, they create complete protection without the blind spots that attackers target. No verification method stands alone. A selfie, a phone number, or a document on it's own can't verify someone's identity. CLEAR1 validates each input, cross-checks signals against each other, and corroborates them with authoritative third-party data — ensuring the person is who they claim to be.

Flexible layers that you control

CLEAR1 gives organizations the flexibility to configure different verification layers for different use cases. For example, businesses might use **Layer 1, Layer 3,** and **Layer 3** for new user onboarding and **Layer 1** for routine re-authentication.

The result: Identity assurance becomes an operational advantage.

With CLEAR1's configurable, interoperable layers that evolve with emerging threats, organizations gain the capacity to tailor verification to specific contexts, scale with confidence, and future-proof their customer journeys without building from scratch.

CHAPTER 3

Multi-Layered Identity in Practice

Real-world implementation transforms multi-layered identity from a concept to your competitive advantage. Three industry leaders — Surescripts, 100, and T-Mobile — demonstrate how different organizations deploy unique combinations of identity signals based on their specific security requirements, compliance needs, and operational priorities. The same underlying system can power entirely different verification strategies for a different use case while delivering consistent assurance.

Proven Implementation Framework

While each organization configures its multi-layered identity approach differently, successful implementations typically follow a common framework:

1. **Assessment:** Before selecting verification methods, organizations evaluate which access points and transactions need the strongest security. This involves analyzing current vulnerabilities and workflow problems to identify priority areas for improvement, then mapping the user journey to determine where verification should occur without disrupting operations.

   Organizations identify key moments that require verification, such as:

   - **Account creation:** Comprehensive checks establish initial trust from day one
   - **Account recovery:** Security and convenience are in balance when restoring access
   - **System access:** Elevated protection safeguards sensitive data

2. **Signal selection:** Based on the assessment, organizations strategically select verification components that reinforce each other. Document validation paired with biometric selfie matching ensures both government ID validity and confirms that the person presenting it is the legitimate owner. Behavioral and contextual signals enable continuous risk assessment without adding friction, while source corroboration validates personal information against trusted databases.

3. **Integration approach:** An organization's implementation strategy significantly impacts both security and user experience. CLEAR1 offers flexible integration options to maintain consistent experiences: native app and web SDKs for direct embedding, turnkey integrations with platforms like Okta, Ping, and Epic, plus enterprise system connections through orchestration partners. Configurable verification thresholds allow risk-based adaptation, while reusable identity components eliminate repetitive verification requirements — users don't need to reupload documents every time, streamlining the process while maintaining security.

4. **Adaptive evolution:** Threats change, so verification methods must change too. Organizations can monitor how well their verification stops current attacks, gather intelligence on new fraud techniques, and update their security layers based on emerging risks. They can also reassess their verification requirements when business needs or regulations change.

Industry Leaders: Configuring Identity For Maximum Protection

The following case studies demonstrate how leading organizations across different industries have configured unique combinations of identity signals to address their specific challenges.

surescripts
Health Information Network™

Healthcare: Surescripts Transforms Provider Verification With CLEAR1

Surescripts powers the nation's leading secure network for prescribing and clinical information exchange, connecting over two million healthcare professionals and provider organizations.

The challenge:

Healthcare networks face a complex identity problem: They need federal-level security compliance while maintaining the speed essential for clinical workflows. With **medical records selling for up to $1,000 each** on dark markets and strict NIST 800-63-3 IAL2 requirements, **Surescripts needed verification** that's bulletproof and user-friendly.[24]

How they configured multi-layered identity:

Surescripts deployed three strategic verification layers to address their specific healthcare requirements:

1. They combined document verification (government ID) with facial biometrics to establish a high-confidence initial identity. (**Layer 1 + Layer 2**)

2. Multi-dimensional source corroboration runs comprehensive backend checks against authoritative databases to government-issued ID and personal information. (**Layer 3**)

3. Liveness detection prevents spoofing attempts, particularly critical when protecting patient data access. (**Layer 1**)

Operational impact:

80%

verification success rate (compared to 41% with their legacy solution)

40%

faster verification process through one-time setup and instant facial recognition for subsequent access

50%

improvement in provider onboarding completion, dramatically reducing abandonment during verification

The healthcare-specific approach:

This configuration demonstrates how multi-layered identity adapts to industry needs. Where financial institutions might emphasize real-time fraud detection, healthcare prioritizes compliance verification and workflow continuity, showing how the same framework serves entirely different operational requirements.

Real Estate: 100 Secures the Rental Application Experience With CLEAR1

100 is a real estate platform that streamlines the rental application process, connecting prospective tenants with multifamily landlords through digital-first experiences.

The challenge:

Real estate platforms face a unique identity dilemma: Rental applications require comprehensive background information while maintaining conversion rates. Applicants abandon lengthy verification processes, but landlords need thorough vetting to protect their assets. 100 needed to balance thorough security checks with a seamless application experience.

How they configured multi-layered identity:

100 took a strategic approach by:

1. **Embedding** identity confirmation within their native application workflow to maintain a consistent user journey. (**Layer 6**)
2. **Deploying** comprehensive verification checks with calibrated pass/fail thresholds to balance security with accessibility.

Operational impact:

- Reduced application abandonment
- Enhanced security without creating barriers to completion
- Strategic utilization of identity data for secondary review and pattern analysis

The real estate-specific approach:

This configuration demonstrates strategic signal utilization. Rather than treating all verification layers as binary pass/fail checkpoints, 100 uses some for immediate security decisions and others for intelligence gathering and secondary review. This approach maintains application completion rates while providing landlords with comprehensive risk assessment data, showing how multi-layered identity can enhance rather than obstruct user experience.

T Mobile

Telecommunications: T-Mobile Enhances Workforce Identity Verification With CLEAR1

T-Mobile connects people and businesses with America's largest and fastest 5G network.

The challenge:

Today's threats include cybercriminals who are outpacing outdated screening and authentication methods, posing as trusted employees to gain access to sensitive systems and data.

T-Mobile recognized that addressing the rapidly shifting threat landscape needed more than stronger passwords or traditional MFA prompts. As a step toward strengthening its security, T-Mobile worked with CLEAR to enhance its identity verification with a solution designed to better keep pace with evolving threats.

How they configured multi-layered identity:

T-Mobile took a strategic, comprehensive approach by:

1. Adding a fast, secure, and scalable biometric MFA layer across its operations. (**Layer 1 + Layer 2**)

2. Partnering with CLEAR1 to analyze signals, from biometrics and documents to devices and trusted sources, to verify that employees are who they claim to be. By cross-checking submitted identity data against authoritative third-party databases, CLEAR1 adds an extra layer of source corroboration that strengthens identity assurance. (**Layer 3 + Layer 4**)

Operational impact:

Enhanced protection against credential theft and social engineering attempts

The telecommunications-specific approach:

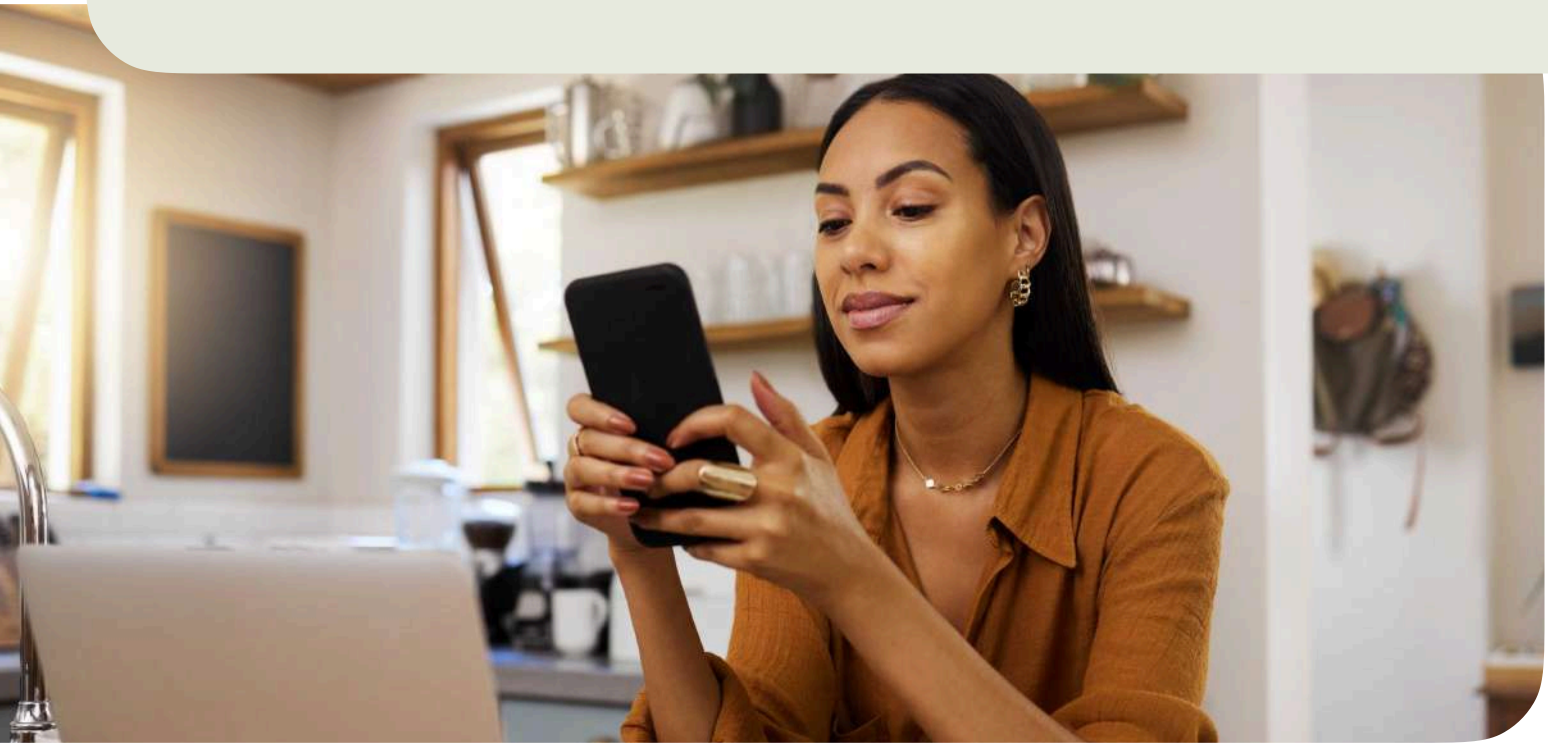
This implementation demonstrates how a multi-layered identity approach can be deployed as part of a forward-looking enterprise security strategy. With CLEAR1's verification capabilities thoughtfully integrated into its existing security infrastructure, T-Mobile's security framework can better keep pace with evolving threats.

Beyond Security: The Natural Outcomes of Strong Identity Verification

When organizations deploy multi-layered identity strategically, security becomes just the starting point. The real value emerges through the natural outcomes that strong identity verification enables across an entire organization.

With a comprehensive approach, businesses can deliver critical benefits simultaneously:

1. **Prevent fraud:** By verifying multiple dimensions of identity, organizations can detect and block attacks before they succeed.
2. **Minimize risk:** The defense-in-depth strategy ensures that even if one layer is compromised, overall security remains intact.
3. **Protect sensitive data:** By ensuring only verified individuals access systems, organizations safeguard their most valuable information assets.
4. **Enable seamless experiences:** Properly implemented, multi-layered identity minimizes friction for legitimate users while maximizing security. It's as easy as snapping a selfie for the users, but in the background, many checks are happening to make it as secure as possible.



CONCLUSION

The Future of Identity Assurance

Identity is Foundational

As organizations recognize that identity is the foundation of digital security, multi-layered approaches have become essential. The most successful implementations balance robust protection with seamless experiences, configuring unique combinations of identity signals that adapt to specific business requirements.

In today's interconnected environment, where digital interactions require absolute trust, this multi-dimensional approach fundamentally transforms how businesses establish confidence in who they're dealing with. Every meaningful interaction, transaction, and relationship depends on knowing with confidence who is on the other end.

CLEAR1: The Complete Multi-Layered Identity Solution

CLEAR1 represents the most advanced identity assurance platform available today.

- ✓ **Multi-layered approach**

  Comprehensive solution that integrates all essential identity signals within a single, cohesive platform

- ✓ **Adaptive verification**

  Configure your identity approach based on context, risk level, and business rules, ensuring security without unnecessary complexity

- ✓ **Highest-fidelity verification**

  Access to a network of more than 31 million CLEAR users* who have undergone the highest level of verification

- ✓ **Enterprise-grade security**

  IAL2, AAL2, and HIPAA compliance that mitigates legal risks as regulations evolve

*Based on CLEAR Q1 2025 earnings report

Identity Matters Everywhere

Your organization faces a fundamental decision: Continue relying on traditional or isolated signal solutions that create vulnerability or deploy comprehensive identity assurance that prevents fraud, minimizes risk, and protects sensitive data while delivering seamless experiences that build lasting trust.

CLEAR1 is all-in on secure identity — delivering the comprehensive solution your business needs to establish absolute confidence in every digital interaction.

Protect Your Business

Connect with our team to explore how CLEAR1's multi-layered approach can strengthen security, enhance your experience, and drive operational excellence.

SCHEDULE A CONSULTATION

[1] Social Security, The Story of the Social Security Number, July 2009 (Accessed July 1, 2025)
[2] ICAO, ICAO Traveller Identification Programme (Accessed July 1, 2025)
[3] ICAO, The Malaysian Electronic Passport, March 1998 (Accessed July 1, 2025)
[4] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, July 2004 (Accessed July 1, 2025)
[5] FinCEN, USA PATRIOT Act (Accessed July 1, 2025)
[6] Department of Homeland Security, REAL ID Act, May 2005 (Accessed July 1, 2025)
[7] Federal Register, Electronic Passport, October 2005 (Accessed July 1, 2025)
[8] Transportation Security Administration, Timeline (Accessed July 18, 2025)
[9] Apple, Apple Announces iPhone 5s — The Most Forward-Thinking Smartphone in the World, September 2013 (Accessed July 1, 2025)
[10] NIST, Digital Identity Guidelines, June 2017 (Accessed July 1, 2025)
[11] Apple, The Future Is Here: iPhone X, September 2017 (Accessed July 1, 2025)
[12] Roll Call, Cleaning Up SolarWinds Hack May Cost as Much as $100 Billion, January 2021 (Accessed July 1, 2025)
[13] NBC News, Cyberattack Cost MGM Resorts About $100 Million, Las Vegas Company Says, October 5, 2023 (Accessed July 21, 2025)
[14] TechCrunch, How the Ransomware Attack at Change Healthcare Went Down: A Timeline, January 2025 (Accessed July 1, 2025)
[15] ISO, ISO-IEC: 18013-5:2021: Personal Identification — ISO-Compliance Driving License, September 2021 (Accessed July 1, 2025)
[16] Deloitte, Generative AI Is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking, May 2024 (Accessed July 1, 2025)
[17] F5, Attacker Economics, December 2020 (Accessed July 1, 2025)
[18] FBI, FBI, This Week: Synthetic Identity Theft, December 31, 2019
[19] Keeper Security, Four Notable Credential-Stuffing Attacks on Companies in 2024, September 2024 (Accessed July 1, 2025)
[20] MIT Sloan Management Review, How Ferrari Hit the Breaks on a Deepfake CEO, January 2025 (Accessed July 1, 2025)
[21] HelpNet Security, 2024 Phishing Trends Tell Us What to Expect in 2025, February 2025 (Accessed July 1, 2025)
[22] Verizon Business, 2024 Data Breach Investigations Report: Executive Summary, May 2024 (Accessed July 1, 2025)
[23] IBM Security/Ponemon Institute, Cost of a Data Breach Report, 2024 (Accessed July 1, 2025)
[24] DOJ, Lithuanian Man Arrested for Theft of Over $100 Million in Fraudulent Email Compromise Scheme Against Multinational Internet Companies, March 2017 (Accessed July 1, 2025)