



CLEAR

WHITEPAPER

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



## Table of Contents

---

### INTRODUCTION

# Identity: The Foundation of Digital Trust

### CHAPTER 1

## Vulnerable by Design: The Risks of Traditional Identity Verification

### CHAPTER 2

## How Multi-Layered Identity Delivers Unmatched Assurance

### CHAPTER 3

## Multi-Layered Identity in Practice

### CONCLUSION

## The Future of Identity Assurance

# 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central importance, our collective understanding of what identity is and how it's defined remains anchored in outdated practices.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.

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



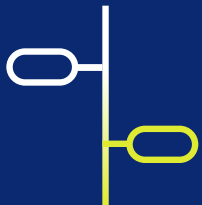
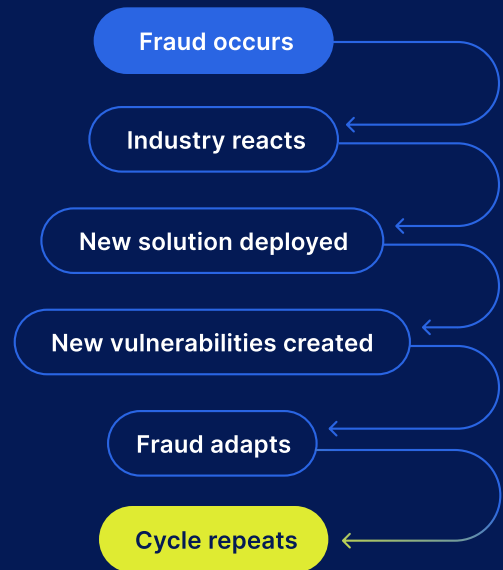
**In this whitepaper, you'll learn:**

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

# 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.




## 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.

### 1980s



### MRZs on travel documents introduced

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

### 1998



### First e-passport introduced

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

### 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.<sup>1</sup>
- Society's understanding of identity becomes tied to a number rather than just physical characteristics or documentation, creating the first widespread numeric identifier.

# 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.

### 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.<sup>4</sup>
- **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.<sup>5</sup>

## INTRODUCTION

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.<sup>6</sup>
- Identity documents become standardized across jurisdictions, establishing the concept that identity verification requires consistent, minimum security standards.

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.

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.<sup>8</sup>
- Identity verification becomes contextual and efficient, enabling pre-vetted, low-risk travelers to experience expedited, less intrusive screening.

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).<sup>7</sup>
- Identity verification begins to incorporate multiple layers (physical document + digital verification), establishing that stronger identity assurance requires verification across different mediums.

2010



### CLEAR launches the secure identity platform

- 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.

## INTRODUCTION

2013



### Consumer biometric authentication introduced

- Apple introduces Touch ID on the iPhone 5S, bringing fingerprint-based biometric authentication into the mainstream consumer experience.<sup>9</sup>
- 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.

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.<sup>12</sup>
  - ▶ **MGM Resorts (2023):** A social engineering cyber attack targeting hospitality operations shuts down casino systems for 10 days, costing the company \$100 million.<sup>13</sup>
  - ▶ **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.<sup>14</sup>
  - ▶ The exploitation of personal data undermines traditional knowledge-based verification, forcing recognition that “secret information” can no longer be considered definitive proof of identity.

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).<sup>10</sup>
- 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.<sup>11</sup>
- 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.”

2021



### MDLs introduced

- States begin adopting mobile driver's licenses (mDLs) as digital complements to physical IDs, with Arizona, Utah, and others leading implementation.<sup>15</sup>
- 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.



CLEAR



## INTRODUCTION

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.

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.

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.<sup>16</sup>
- 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.

2025

# 1 CLEAR1 sets the new standard in identity by expanding NextGen Identity+ to 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.



Fill out the *form*  
below to keep reading

