White Paper

Identity Verification: Enhancing the Customer Journey

Dilip Singh, Jie Liu
Equifax D&A

April, 2025

Contents

Executive summary

Identity Verification: Enhancing the Customer Journey
In today's digital-first world, digital identity verification plays a pivotal role in securing and verifying everything from onboarding new accounts to facilitating payments and other critical transactions. Establishing trust through accurate identity verification forms the foundation of successful business-customer relationships. However, traditional methods of digital identity verification often pose significant challenges, including prolonged processing times, increased fraud risks, and frustrating customer experiences. These issues result in higher abandonment rates, greater exposure to fraud, and lower overall customer satisfaction.

Equifax addresses these challenges with its industry-leading database of consumer identity records. By leveraging cutting-edge artificial intelligence (AI) and machine learning (ML) technologies, Equifax delivers a precise, data-driven identity verification solution: **Equifax Digital Identity and Trust**.

This white paper explores evolving business needs for more secure and efficient identity verification solutions. It introduces Equifax Digital Identity and Trust, highlighting how its capabilities can be customized to meet a variety of business challenges. We also examine how organizations of all sizes can benefit from this innovative solution, discuss best practices, and provide guidance on evaluating and implementing identity verification strategies effectively.

Introduction

The process of identity verification has undergone significant evolution, shifting from manual, paper-based methods to advanced, technology-driven approaches that prioritize accuracy, speed, security, and user experience. This transformation reflects the growing demand for secure and seamless identity verification in today's increasingly digital environment.

For many organizations, enhancing identity verification processes remains a strategic priority. Businesses recognize that leveraging more data points and establishing stronger data linkages can significantly improve the accuracy and reliability of their verification systems.

As digital transformation accelerates, the time is right for businesses to adopt innovative solutions that offer more advanced and reliable identity verification capabilities. Meeting the evolving needs of both businesses and consumers requires a comprehensive, data-driven approach that balances security with customer experience.

The primary purpose of most identity verification products is account protection, encompassing account logins, new account creation, and account takeover prevention. Additionally, identity verification plays a critical role in meeting regulatory and compliance mandates such as Know Your Customer (KYC) and Customer Identification Program (CIP).

With the increasing threat of personal data breaches, synthetic identity fraud, and account takeovers, businesses must adopt more robust solutions. Customers now expect more than fragmented systems that combine disjointed personally identifiable information (PII). Instead, linking digital identity attributes with traditional physical identity markers creates a more comprehensive identity profile, effectively reducing fraud risk in digital transactions.

However, transitioning from legacy identity verification products to modern solutions can present several challenges. Common obstacles include:

1. Data migration
2. Integration challenges
3. Cost and resource constraints
4. Product training and understanding
5. Business process and goal alignment
6. Use case and configuration adjustments
7. Platform migration and technical complexity

Despite these challenges and difficulties, the advantages of adopting a next-generation identity verification product are substantial. In today's digital-first economy, implementing a more advanced identity solution is essential.

In the following sections, we will introduce and discuss **Equifax Digital identity and Trust (DIT)**, exploring how it addresses these challenges while delivering robust, scalable, and customizable identity verification solutions.

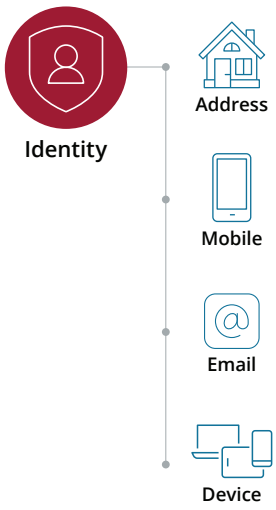
A better, stronger, high-performing product

Voice-of-customer (VOC) insights revealed a desire for a more robust identity verification product. To address this, Equifax developed a next-generation solution: **Digital Identity and Trust**. By leveraging comprehensive reference data sources and an expanded set of PII data elements, DIT delivers enhanced population coverage, higher verification accuracy, and improved identity decision-making. These capabilities are supported by advanced AI/ML models, robust identity graphs for data linkage, and intelligent verification rules and strategies.

1. More PII data elements

Traditional identity verification relies primarily on physical identifiers such as addresses and Social Security Numbers (SSNs). The DIT product goes beyond these static data points by incorporating dynamic digital identifiers, including email addresses, mobile phone numbers, device IDs, and IP addresses. A considerable number of organizations face limitations in their ability to access and analyze IP and email data, where both of them are critical factors for accurate identity verification. By maximizing the use of diverse PII elements, Equifax DIT enhances verification accuracy and strengthens decision-making processes.

Figure 1: PII data elements



2. Enhanced population coverage

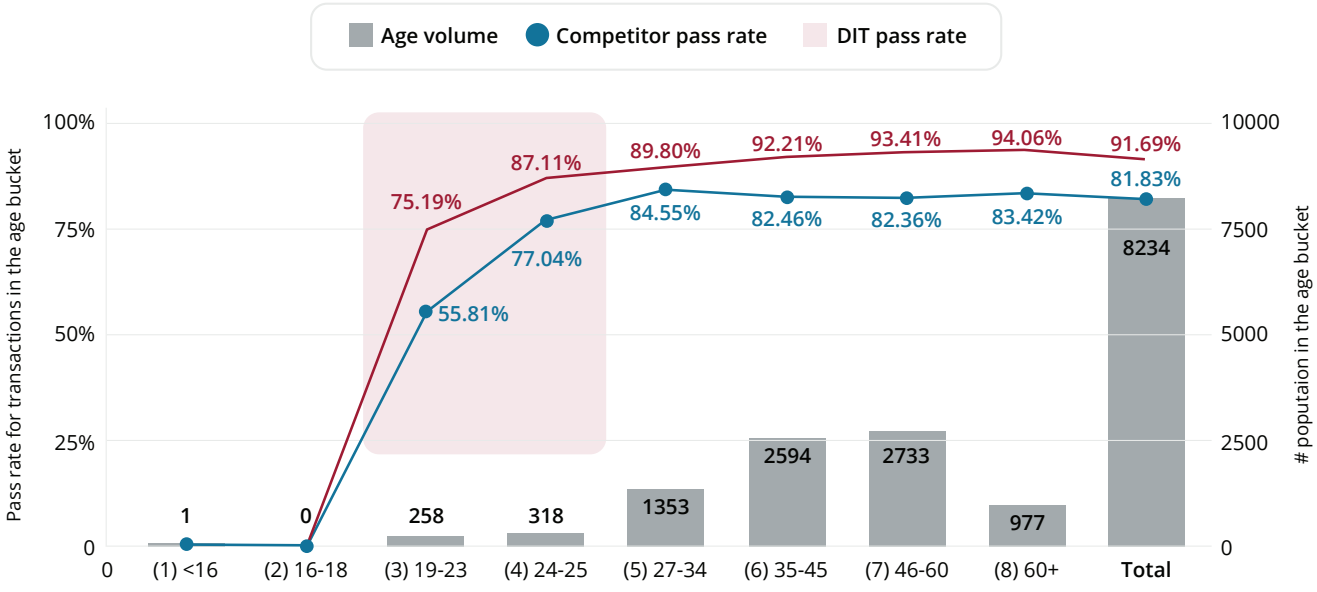
Effective identity verification requires broad coverage across diverse populations. With differentiated, multisource data, Equifax DIT routinely achieves population coverage rates greater than 98%, ensuring high verification success across most customer transactions. Comprehensive customer analyses and reference data hits further validate this performance, ensuring businesses can securely verify nearly all potential customers.

3. Strong coverage for younger populations

Verifying young or underbanked populations — particularly individuals aged 18 to 26 — has historically been challenging due to limited credit or banking histories.

Equifax DIT addresses this gap by leveraging multisource data to improve coverage rates in this age group. Compared to legacy identity verification products, DIT passes 50% more transactions for younger populations[1], providing businesses with a competitive advantage in reaching this critical demographic segment.

Figure 2: DIT passes more transactions in young age group



[1] Conclusion derived from a comparison study between Equifax's legacy product, i.e., Equifax ID (EID) vs Equifax DIT based on a group of customer analysis.

4. Advanced identity graph for PII linkage

The Equifax DIT identity graph connects both traditional and digital identity elements, creating a comprehensive and cohesive identity profile. Traditional PII data elements, such as driver's licenses, passports, and utility bills are seamlessly linked to digital identifiers like email addresses, phone numbers, geolocation data, and device IDs.

The identity graph establishes meaningful relationships between these elements — for example, linking a name to a phone number or matching an IP address with a physical location. Inconsistent or mismatched data can signal potential fraud risks. By combining physical and digital identity data, DIT delivers unparalleled identity insights while preserving data integrity within its identity graph framework.

Figure 3: Equifax DIT identity graph

5. High performance

Equifax DIT consistently outperforms the legacy EID product, passing 20% more transactions while reviewing fewer accounts - all with comparable risk exposure. Recent customer use case studies demonstrate identity trust rates ranging from the low to mid-90% range. An impact and fraud analysis revealed DIT drove a 38% reduction in charge-offs while maintaining similar net margins on quality bookings.

Product and proof of concept testing

As highlighted in Section 1, Equifax has introduced a next-generation identity verification and authentication solution: **Digital Identity and Trust (DIT)**. This product is continuously evolving, leveraging cutting-edge AI/ML models, updated data sources, and risk signals to adapt to emerging business needs. Ongoing enhancements help position DIT as one of the industry's leading identity solutions.

Equifax DIT uses both physical and digital persona data linked to a specific identity for a comprehensive, multidimensional verification assessment. For each transaction, DIT analyzes a combination of PII data elements, generating trust responses for each.

These assessments cover key identity-related capabilities, including affiliation analysis, identity verification, and risk signaling. This robust evaluation process comes together to deliver strengthened trust definition, enabling businesses to make even more informed decisions. For more information on DIT's capabilities, contact the **Equifax Product Team**.

While DIT provides powerful verification capabilities, businesses can enhance their identity protection strategy by integrating add-on solutions. These could include Secure Multi-Factor Authentication (MFA) or our new Dynamic Knowledge-Based Authentication (KBA). These solutions can be deployed as additional security measures when transactions require extra verification or when initial verification attempts fail.

To ensure optimal product performance, the Data & Analytics (D&A) and Operations (Ops) teams collaborate to provide automated customer testing with a fast turnaround time. The DIT Proof of Concept (POC) testing process follows these key steps:

1	2	3	4
Customer data preparation	Secure data transfer	DIT testing	Performance analysis and results delivery

Among these steps, customer data preparation is especially crucial, as input data directly impacts DIT's effectiveness. To gain deeper insights into product performance, Equifax encourages customers to include risk indicators, bad signals and revenue/loss amounts during testing. This enables a more comprehensive impact analysis, highlighting both potential gains and areas for improvement.

Figure 4: Personally identifiable information (PII) verifiability chart

Identity inputs & identity trust - Do we trust the inputs provided?							Overall recommendation based on inputs received		
Name (Required)	Address (Required)	Date of birth	SSN (Full or partial)	Email address	Phone number	Expected identity trust rate*	Approve	Review	Deny
✓	✓					Low 80's	Not possible	Possible	Possible
✓	✓	✓				Low / Mid 90's	Not possible	Possible	Possible
✓	✓		✓			Low / Mid 90's	Possible	Possible	Possible
✓	✓			✓	✓	Low 90's	Possible	Possible	Possible
✓	✓	✓	✓	✓	✓	Mid / High 90's	Possible	Possible	Possible

Guiding customers in providing input data

Accurate identity verification depends on the availability and quality of personally identifiable information (PII). An input impact analysis conducted by the Equifax team in 2022 confirmed that providing a wide range of PII elements improves the system's ability to assess the trustworthiness of an identity. To ensure a minimum standard for verification, Equifax requires customers to submit at least two essential PII elements: Full Name and Physical Address. These foundational details enable DIT to perform its initial identity verification checks. However, a single PII input is insufficient for reliable assessments. Customers are encouraged to provide as many relevant PII elements as possible to enable the system's models to generate more accurate verification results.

PII validity is equally important. The PII validation process by Equifax evaluates the accuracy and reliability of submitted data through multiple checks. It also analyzes PII distribution, such as age demographics, to detect unusual patterns. Additionally, DIT performs velocity checks to identify repeated transactions using the same PII elements. A high frequency of shared PII usage could signal potential misuse, fraud attempts, or compromised records. These validation steps ensure trustworthy and reliable POC testing for customers by verifying both the quantity and quality of submitted PII data — a hallmark of the effectiveness of our DIT product.

Figure 5: PII validity elements

Social Security Number (SSN)...

- cannot be missing.
- cannot have 000 in the area field (digits 1-3).
- cannot have 00 in the group field (digits 4-5).
- cannot have 0000 in the serial field (digits 6-9).
- cannot have 666 in the area field (digits 1-3).
- cannot start with 9.
- full SSN needs to be exactly 9 symbols and all of these symbols are only numeric fields.
- full SSN (digits 1-9) cannot be in the invalid list.

Date of Birth (DOB)...

- birth year should be after 1900, before year of today.
- birth month should be 01-12.
- birth date should be 01-31.
- full DOB should be smaller than today.

Conclusion

While many organizations have yet to reach their ideal identity verification standards, the accelerating pace of digital transformation has motivated them to pursue modernization and migration towards more advanced solutions.

Whether they are long-standing Equifax customers or new clients, businesses can benefit from this powerful and innovative identity verification product. Powered by differentiated and multisource data, advanced data linkage and affiliations, AI-driven models, and configurable verification strategies, Digital Identity Trust (DIT) is designed to meet evolving industry needs.

Equifax has built a strong track record through proven use cases and customized solutions. A recent product upgrade successfully resolved the energy sector's longstanding challenge of maintaining accurate address records. Additionally, we continuously refine DIT's performance by incorporating customer-provided fraud and risk signals, ensuring high accuracy with minimal revenue impact.

Adapting to change is essential for growth and success. Now is the time to embrace innovation and take identity verification to the next level.