EQUIFAX ®

Digital Identity Trust

Identity verification you need with results you can trust

No business is immune from identity fraud. Digital Identity Trust (DIT) from Equifax gives you the confidence you need and results you can trust with our proprietary three prong evaluation methodology to verify identities that help you mitigate fraud.

Step 1

Acceptance of up to seven (7) physical and digital identifiers

Digital Identity Trust allows you to input up to seven (7) identifiers to give you a high level of confidence in a consumer identity in a way that works with your established inputs. Both physical and digital identifiers can be accepted including:

| Address | Social Security Number | Name | Device | Phone | Date of Birth | Email |

Step 2

Each input is evaluated using a three-pronged methodology and assigned a trust value

A Yes/No trust value is given to each input received using the three pronged methodology. The three levels of evaluation are below.

TRUST
Trust is the net balance between positive and negative indicators for overall confidence in the PII Identity.

INSIGHTS
Additional profile, facts or supporting info regarding the PII element with or without other elements.

AFFILIATION
Connections/associations/links between the particular PII element and other PII elements.

VERIFICATION
Confirms whether or not that data element exists.

Digital Identity Trust At-A-Glance

Features

- Up to seven (7) identifier inputs
- Evaluates traditional PII as well as digital signals including Email, Phone, and Device/IP
- Proprietary methodology for evaluation of submitted identifiers
- Recognizes multiple verification attempts with Pattern Recognition
- Can be orchestrated with step up authentication including Dynamic KBA or Secure Multi-Factor Authentication (SMFA)
- Allows for add-ons of regulatory and compliance information to assist with KYC efforts

Sample Use Cases

- Account Opening
- Loan Origination
- Account PII Changes
- KYC Efforts

Accessibility

- Direct API
- Global Batch Processing
- InterConnect API, Batch, and UI
- User Interface

powering the world with knowledge ™

Step 3
Finally, we corroborate the trust values of each input and provide you with a recommendation

We not only evaluate the identifiers provided on input, but we provide a recommendation based on the data we see. Along with the trust values and findings, we give you a recommendation to **Approve** the consumer, **Review** the consumer, or **Deny** the consumer based on the information received.

DIT is packaged in a way to best meet the needs of your business

When selecting DIT, you have two options - DIT Core and DIT Enhanced.

1. **DIT Core** - Evaluation of Traditional PII identifiers including Name, Address, DOB, and SSN

2. **DIT Enhanced** - Evaluation of Traditional PII identifiers PLUS digital signals including Phone, Email, and Device/IP

Digital Identity Trust Available Add-Ons

We also allow you to add on additional features based on the needs of your business. The options below can be added to either DIT Core or DIT Enhanced:

1. **Dynamic Knowledge Based Authentication (KBA)**
   Dynamic KBA allows you to take the identity verification DIT provides one step further by adding a step up authentication option using questions of the consumer only they should know. Questions that are served up to the consumer when added on to DIT include tradeline, non-tradeline, and employment questions.

2. **Regulatory Package**
   The Regulatory Package provides additional reason codes and short descriptions to help you meet KYC requirements. Example reason codes included in the Regulatory Package are "FX - Fraud Victim Long Term Fraud Alert", "85 - SSN was never issued or issued after June 2011", or "90 - SSN reported as deceased".

3. **Reason Code Extension**
   The Reason Code Extension Package provides an additional set of reason codes and short descriptions that extend beyond those provided within the Regulatory Package. Example reason codes include "3A - The current address is a PO Box Address", "4N - Date of birth is validated", "64 - Phone Number not validated".

4. **OFAC Reason Codes**
   OFAC reason codes are available to assist with customer due diligence (CDD) by providing up to 13 flags available from OFAC. Example reason codes include "01 - Foreign Terrorist Organization", "ON - No Match on OFAC", or "02 - Specially Designated Narcotics Trafficker".

For more information about Digital Identity Trust from Equifax, contact your sales representative.

equifax.com/business