IdentityMind™ GLOBAL

Digital Identities You Can Trust

Trusted Digital Identities

WHITE PAPER

Share

www.IdentityMindGlobal.com

Introduction

Today there are large-scale data breaches almost every quarter and a proliferation of websites where you can buy identities including a name, email address, phone number and SSN for about a dollar. At the same time, FinTech companies and Financial Institutions are trying to onboard as many customers online as quickly as possible. In this new environment, preventing fraud, money laundering and the financing of terrorism is no longer just about knowing whether an identity is real, but knowing whether the identity belongs to the person using it and whether you can do business with that identity.

Bank Secrecy Act (BSA) regulations mandate Customer Identification Programs (CIP) as one of the pillars of Anti-Money Laundering (AML). The BSA also mandates that FI's must risk-rate their applicants, and apply enhanced due-diligence (EDD) for higher risk clients. The question is how to establish the risk rating of an identity solely based on the information provided, when such information can be reasonably easy to acquire, especially to those who have the means and the motivation to do so.

Establishing that an applicant is who they say they are and evaluating all of their entities (e.g. email addresses, physical addresses, credit cards, devices) against various risk indicators, including affiliations and connections to verifiable sources of risk, is the basis of Trusted Digital Identities™ (TDI™).

Digital Identity Validation

There is clear value in performing identity validation beyond compliance. The more certain you are about dealing with a real identity, the better you understand the risk involved in a transaction. In order to validate an identity online there are many options. There are third party databases, such as IdentityMind (IDM), to validate that the applicant's information have been seen before. You may also use social networks, deep web searches, etc. If there are inconsistencies in the data, you can perform EDD such as Out of Wallet Questions / Knowledge Based Authentication. Some FI's incorporate document verification (specifically in countries that welcome it such as Germany and Canada) as well as biometrics.

Risk Beyond Identity

There are many ways to measure applicant risk:

IP and Device Information

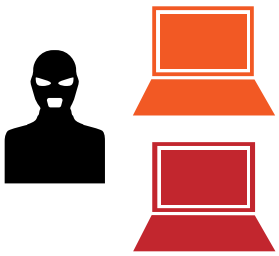
There is a component of risk that can be measured through IP address analysis and the device information (e.g. device fingerprinting). For many FI's, the use of proxies (both anonymous ones and simply those with a bad reputation) is their largest risk indicator, while for other FI's it is the distance between the location of the IP address and the billing address. For most FI's, it is a combination of both.

Fraud rates are 15x higher when the user's billing address and IP geolocation do not match.

https://www.internetretailer.com/2005/01/06/how-geolocation-can-reduce-the-risk-of-online-fraud

Multiple Accounts

The creation of multiple accounts in a small timeframe is strongly associated with fraudulent activity. For users that have or are the beneficial owners of multiple accounts, tracking their activity to determine if you want to continue the relationship is key.

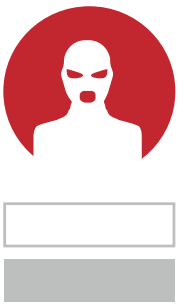


Account takeovers and fraudulent account creation grew 124% between Q4 2014 and Q4 2015.

https://www.miteksystems.com/sites/default/files/docs/Account-Takeover-and-Creation-Fraud-CNP-White-Paper-Final_0.pdf

Application Risk

This risk should be measured by product line, location, volume, and amount. For example, with digital wallet providers the time between account creation and first transaction is a clear indicator of fraud. Likewise crowdfunding sites have a high correlation between applicants who fund themselves and fraudulent activity.



Find behaviors associated with fraud in your business model, and stop them with waiting periods or other rules.

Regulatory

Sanctions lists prevent you from doing business with countries, individuals and organizations. In addition, you must screen for Politically Exposed Persons (PEPs), often both domestic and foreign.

In 2015, the average dollar amount of an OFAC penalty was $39,980,400.

https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/2015.aspx

Trusted Digital Identities™ (TDI™)

If you are a bank, an online lender, a digital wallet provider, a money remitter, or almost anyone in the FinTech world, then you are wrestling with how to provide a great online experience and expand your client base, while reducing risk and maintaining compliance.

IdentityMind set out to address those risk and compliance needs by answering two fundamental questions:

1) **How to create unique digital identities based on an individual's online attributes and behaviors**

2) **How to aggregate an individual's online financial / payment behavior in order to predict the risk of doing business with that individual**

Fast forward several years, many platform innovations, and many strategic data partnerships, and we have built the capabilities to categorically answer these questions.

A TDI is an identity that is real, that doesn't have a history of fraud or potential money laundering, and that isn't associated with nefarious organizations. Let's discuss how the IDM platform addresses each one of these areas in detail.

Electronic DNA™ (eDNA™): A Real Digital Identity

The core of our technology is a set of data structures and algorithms that represent a digital identity and the risk of that digital identity.

Digital identities are entities that perform transactions online. These entities may be individuals, businesses, affiliates, and others. Let's break this down.

Imagine that Joe Smith is signing up for a digital wallet. In order to open that account, Joe has to provide personal information such as an email address, phone number, billing address, etc. But, “online” Joe is much more than those attributes. He also has several internet-enabled devices, a consistent IP address and location associated with each transaction, payment instruments that are loaded into his digital wallet, physical shipping addresses, and more. Correlating all these attributes and keeping track of the transactions in which these attributes appear is still the easy part.

We know that many individuals have several email addresses, several devices, and maybe even multiple internet identities. Joe has profiles at different dating sites, and social networks. Some are mundane, but some may be used to secretly follow extremists or extremist groups. This is where things start to get messy, technically speaking. An individual in the digital world is a mesh of profiles and attributes. It is a collection of “simple” identities. This collection is what we call the entity's eDNA.

eDNA is more than a large database of correlated parameters. There are many Joe Smiths, Juan Garcias, or Mohammed Abduls on the Internet. eDNA knows how to distinguish among them. eDNA is very careful in how these correlations are established to make sure it is the Juan Garcia you want to look for, and not another one.

Furthermore, eDNA is able to isolate the cases where credit card fraud or identity theft have led to a card or identity being compromised. The last thing you want is to associate Joe Smith's eDNA with the eDNA of the fraudster that stole his card.

The problem to solve is how to keep an entity's eDNA relevant and accurate. How many smart phones have you had in the last 10 years? How many credit cards have you had? The answer to both is likely a large number. eDNA is constantly aging these attributes that are clearly not in use.

eDNA is dynamic: it evolves in realtime and is always up-to-date. An entity's eDNA is the most up-to-date digital representation of an identity.

What makes eDNA fundamentally different from other digital identity technologies are the number of attributes that it tracks and the knowledge about how those attributes are used together in online transactions. Other digital identity solutions focus on a very limited set of attributes and lack the ability to track how those attributes are used together in financial digital transactions. Many focus on a single given identity parameter like device, name, or date of birth. This approach hinders the ability to spot identity theft or compromised accounts, as the identity attributes are not evaluated together.

In this example, fraudulent use of a credit card may occur undetected in the typical solution because the credit card is only linked to the owner's billing address - an identity thief would only need the credit card number and the address to fool this system. eDNA intelligently tracks and associates dozens of attributes so you always know who is performing a transaction. In order for a transaction to pass muster, the credit card would need to be used with not only the correct billing address, but with a known device or email address as well.

Reputation

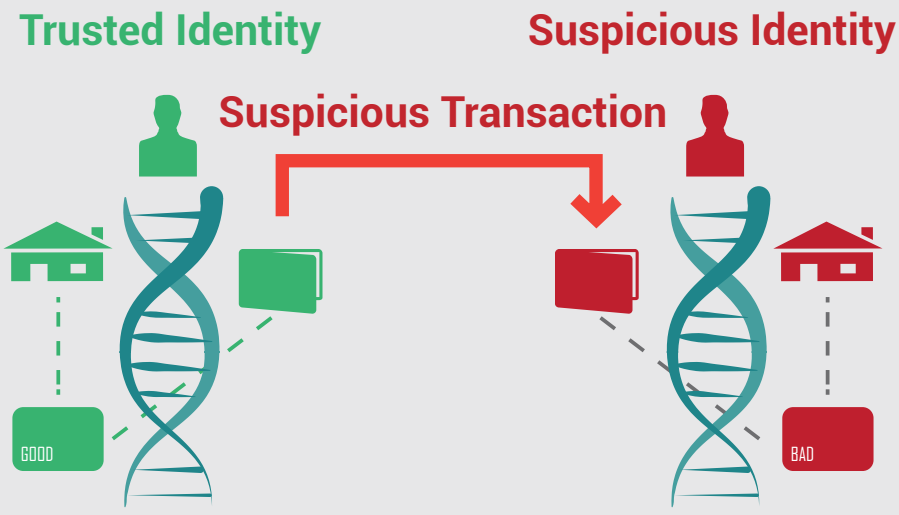
After confirming an identity, the next question is whether you should be doing business with this individual or company. In order to make that decision you have to assess the risk they represent to your institution.

Each organization has a different risk tolerance, depending on the product line, their business model, and the specific regulations they need to comply with. For example, remitters and e-commerce websites have different risk models, as do orders of $10 and $10,000 - even when both orders are from the same company.

In the IDM platform, the riskiness of a transaction is evaluated first and foremost on the reputation of the entities involved. For example, in a remittance transaction between two individuals, the overall risk of the transaction includes the reputation of both source and destination entities.

The reputation of an identity is calculated in real time based off heuristics, the attributes' individual reputation, and the transaction attributes relation to each other.

The combined attributes that define an identity (eDNA attributes) result in an individual reputation score. This score is the aggregation of the behavior of those attributes in the context of online transactions (which include payments, transfers, and online onboarding). The score is defined by the history of the attribute, feedback from trusted third party and authoritative sources, internal heuristics, and the feedback from the financial organizations and merchants evaluating the particular transactions where these attributes are used.



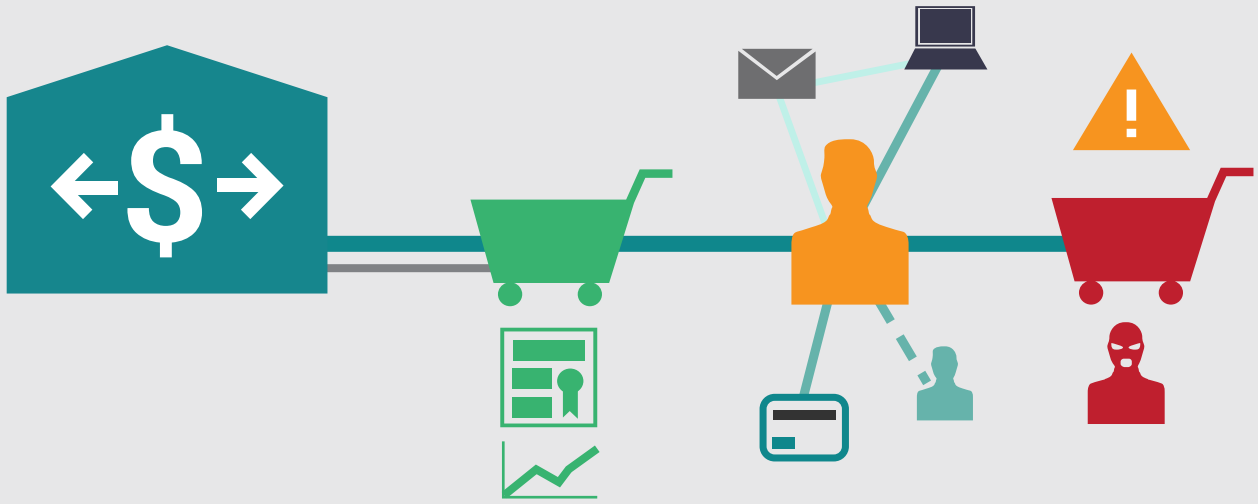
In this example, there is a Trusted Identity making a transfer from a digital wallet to a digital wallet belonging to a Suspicious Identity. The Trusted Identity is considered as such because it is associated with attributes that have been used consistently before with no history of fraud. But the destination wallet of the transaction contains cards that have been previously associated with fraud, and the wallet itself does not have validated funding source. Even though the transaction is being initiated by a Trusted Identity, the system deems the transaction suspicious because the destination is suspicious. If the trusted identity continues to have relationships with suspicious ones, eventually its reputation would drop and it would become suspicious itself.

Affinity and Affiliation

The next part of the puzzle is how these entities are connected to high-risk entities. For example we often see cases where an the entity may not be involved in risky or fraudulent situations, but is associated with entities that have. Imagine you are a Payment Service Provider (PSP) offering payment services to an online merchant. The business itself may be sound, but if you learn the owner has past businesses that closed because of fraud, you will change reserve amounts, how much processing volume you allow, or if you actually onboard that merchant at all.

Your risk evaluation would also change if you knew the person to whom you were about to offer a loan happened to be a Facebook and Twitter follower of terrorist organizations. Or if the person was a known associate of individuals that were affiliated with nefarious organizations.

During the evaluation of entities, the IDM platform can evaluate not only the entity in question but, also its associations. Some of them already established within the IDM database, others through accessing real-time data partners. Either way the evaluation will indicate if these conditions exist.



In this example, a PSP is onboarding a new merchant. The merchant's online store seems safe. But an analysis that stops here misses potential risks. eDNA gives enhanced visibility by looking at the associations of the owner of the online merchant. It finds that the owner has had other business before that have been shut down due to fraud. This increases the risk of an otherwise sound business.

Weave™: Enhanced Sanctions and PEP screening

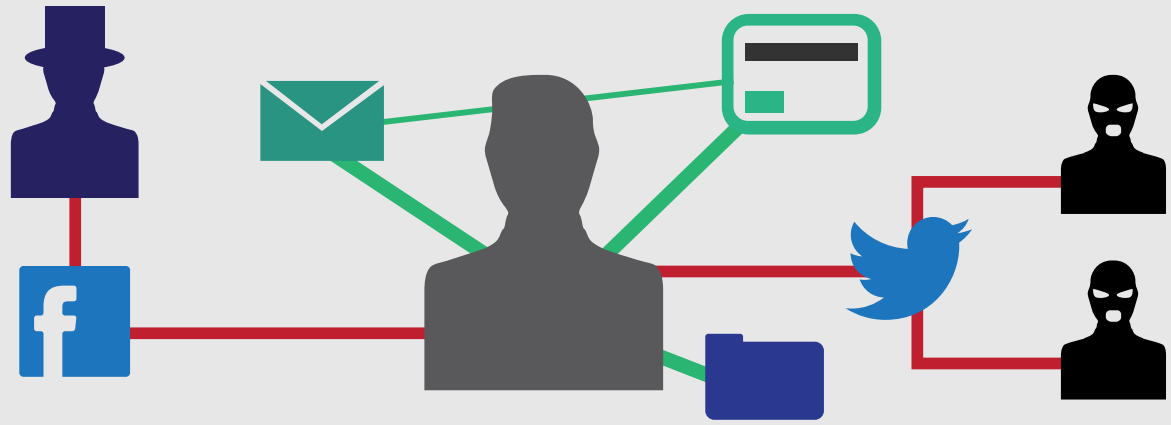
Sanctions lists are issued by different agencies and governments, both domestic and international. Politically Exposed Persons (PEPs) must be screened for, but are not centralized in a single list. PEPs are individuals at a higher risk of money laundering, *and* their known associates. As FinTech companies expand their client base internationally, they need to comply with multiple sanctions lists as well as screen for PEPs from multiple countries. There are examiner findings and regulatory fines if your compliance program doesn't incorporate a rigorous screening of clients against sanctions lists and PEPs, as well as an important amount of direct financial risk.

The major problem with sanctions screening is the sheer amount of false positives. Every potential match takes time to resolve, and some can take hours to address properly. Other providers have false positive rates of over 10%, with dozens of individuals to review for each match. Taking an identity-based approach is a faster and better way to deal with this problem. The more you know about the identity, the easier it is to manage the potential match. At the end of the day we are trying to figure out whether the person you are dealing with is actually a sanctioned individual or a PEP.

Because of eDNA we can simultaneously analyze tens of attributes to quickly discern the probability that a specific individual is a true match to a sanctions list. Furthermore, we can use all of an applicants associations to make sure they have no connections to individuals or businesses that are sanctioned or PEPs themselves.

Identifying the financing of terrorism is difficult because it may not be performed by known “bad” individuals but rather by “normal” citizens who try to inconspicuously funnel smaller amounts of money to nefarious individuals or organizations.

Weave is enhancing screening of lists and PEPs using the eDNA associations. It is leveraging social networks, deep web, and other sources to tag and annotate the extent of an individual's network to better inform the vetting process and streamlining the Enhanced Due Diligence (EDD) process, making it both more efficient and more reliable.



The identity in this example appears to be an overall average user with no fraudulent history of his own, however he is Facebook friends with the mayor of the city he lives in and follows several organizations on Twitter that have been sanctioned by the government. These social network activities in combination with his relationship to Government Sanctioned organizations raises this risk profile.

Trusted Digital Identities in Action

The IDM platform provides a much needed Digital Identity Layer to Financial Services. This layer is accessible through APIs and can be deployed as a SaaS or as an on-premise solution. Leveraging an API, this layer powers the usage of TDI for Fraud Prevention, KYC, Sanctions Screening, Enhanced Due Diligence and Transaction Monitoring to prevent and detect Money Laundering. The platform offers all the necessary tools to efficiently operationalize these functions.

These are the results our clients are benefiting from by using IDM's platform:

60%

Reduction of Transactional Fraud

After a short period of usage, our clients are able to reduce their current chargebacks, on average, by **60%**.

85%

Reduction of Manual Review Time

The current industry average for manual review rates is about 22% of payment transactions. Our clients experience between **3% and 7%**.

90%

Reduction of Onboarding Fraud

The combination of account origination fraud prevention, KYC and Sanctions Screening are a strong combination to prevent or rapidly detect account origination fraud. Some of our clients have expressed IDM has virtually eliminated their account origination fraud.

50%

Reduction of False Positives in Sanctions Screening

One of the highest operational compliance burdens is dealing with the amount of false positives from the sanctions screening process. It is well known that the number is close to 99%. Our platform offers many ways to reduce false positives and to tune the matching algorithms. The TDI information of both the identities evaluated and those in sanctions and PEP lists allows for multi-attribute comparison.

Trusted Digital Identities Can Help Your Business

We're the leading provider of digital identity data, and we're happy to show you why through a Live Demo of our platform. You'll see:

- Our selection of 80+ identity verification tests for Know Your Customer (KYC) applications. Our KYC services offer worldwide coverage.
- Integrated Sanctions Screening. Automatically verify every user against more than 25 sanctions lists. Our Sanctions Screening service is proven to help companies reduce false matches by 50%, as well as reduce the operational costs associated with the process.
- Extensive fraud prevention policies. Our fraud policies can be run during the account creation process to help you prevent fraud losses.
- Our #SuperiorAML program. Detect money laundering schemes using our Anti-Money Laundering (AML) rule builder. The IdentityMind AML engine is further reinforced by our automated Suspicious Activity Report (SAR) function, which allows you auto-fill fields and directly file reports from our platform.
- Increased visibility. Gain insight into good and bad actors with our eDNA™ database of user identities and reputations. The IdentityMind™ network of over 200 million identities is updated in real time.
- Visual analysis. Explore our eDNA™ technology in detail, and see how we visually correlate multiple parameters for every user identity with our Entity Graph.

IdentityMind Global can help you comply with regulations anywhere in the world, protect your bottom line, maintain banking partnerships, and more importantly, safeguard your company's reputation.

To schedule your demo, reach out to us at **sales@identitymind.com**.

If you have questions or comments about this use case, or would like to see other use cases, feel free to contact us through twitter at **@identitymind** or email us at **evangelist@identitymind.com**.