IdentityMind™ GLOBAL

Digital Identities You Can Trust

WHITE PAPER

The Digital Identity Evaluation Guide

Share

www.IdentityMindGlobal.com

Introduction

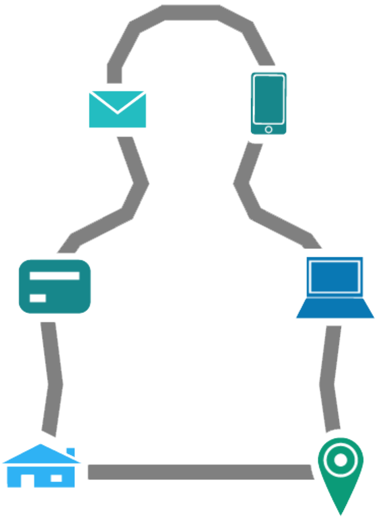
The goal of almost every business is to gain more customers and generate more revenue. The Internet enables businesses to find new customers, both domestic and international. While ecommerce has done this for decades, Financial Services institutions are still catching up. The rise of the FinTech sector over the past five years has been led by firms using the Internet to transform how they attract, interact, and validate potential clients.

Financial Services organizations are different from ecommerce merchants in that the risk of new customers is potentially much higher, and must be mitigated appropriately. Achieving a balance between global customer acquisition, risk assessment, and regulatory compliance, is difficult without the proper strategy and technology.

The following guide provides a framework that will help you think through this strategy highlighting the functionality and technology that can help you achieve it.

Digital Identity Evaluation

Regardless of the details of the strategy for customer acquisition vs risk, it boils down to the data that you collect during onboarding, and what you do with it. This guide will refer to data collection as the Digital Identity of your customer. A Digital Identity can refer to an individual or a business.



A Digital Identity can include: name, email, phone, billing and shipping address, date of birth, social security number, IP address, device fingerprint, passport, government identification, social network handles, etc.

How much data you collect and how you collect it is directly related to the three aspects of the strategy:

Customer Acquisition

Regulatory Requirements

Risk Reduction

Generally, the more information you ask for during the onboarding process, the higher the client abandonment rate. This is as true in financial services as it is in ecommerce. However, in the case of financial services, customers are more patient and are prepared to go through a more rigorous onboarding process. Nonetheless, every customer expects a good user experience and not to be bothered beyond what they consider reasonable. From a customer perspective, what to expect depends on demographics and product type. Millennials have a very different set of expectations than their previous generations when it comes to which information they're willing to share to sign-up for financial services.

Considering the balance between friction and customer acquisition, one of the major considerations is how many Digital Identity attributes you need to collect, how you collect them, and when in the onboarding process you collect them.

There are four fundamental questions to answer when onboarding a client:

1. Is the Identity Real?

You need to prevent synthetic identity fraud where an identity appears to be real, but is not.

2. Is the Applicant the Owner of the Identity?

You need to prevent identity theft and vulnerable victim fraud.

3. Can you do Business with the Identity?

You need to ensure that regulations don't prohibit or prevent you from onboarding this customer.

4. What is the Risk Posed by the Identity?

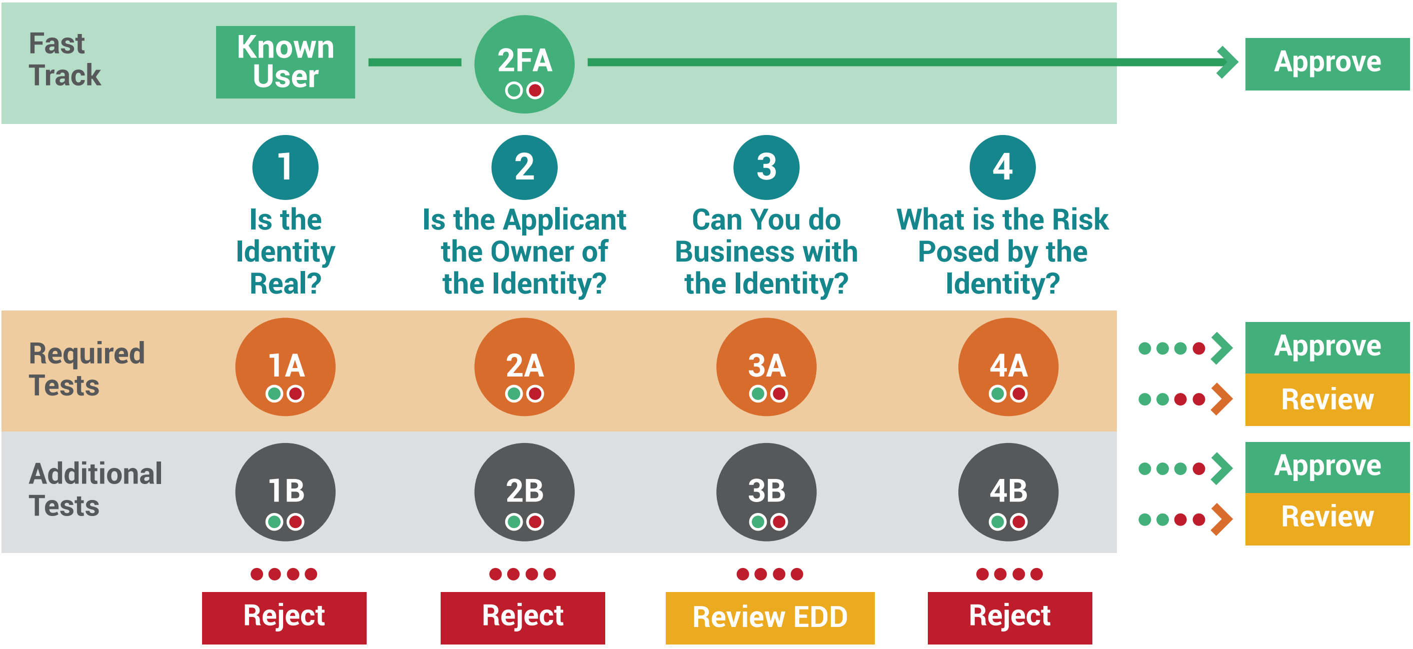
You need to categorize the risk this identity represents to you, within the context of your risk assessment.

The faster you can answer these questions, the faster you can safely onboard a client.

For an analysis on how IdentityMind builds digital identities using our core eDNA™ technology, **click here to download our white paper on Trusted Digital Identities™**

Digital Identity Evaluation Map

The following map, based on the four necessary questions from the previous page, provides the process for verifying digital identities during the onboarding process. Each section contains tests that the user will either pass or fail. While no two businesses are the same, considering the ratio of total passes to total fails can help you inform whether the user should be approved or marked for review. A user can also be rejected for failing too many tests in any one column.



Fast Track: Known User — 2FA → Approve

1 Is the Identity Real?

2 Is the Applicant the Owner of the Identity?

3 Can You do Business with the Identity?

4 What is the Risk Posed by the Identity?

Required Tests: 1A, 2A, 3A, 4A → Approve / Review

Additional Tests: 1B, 2B, 3B, 4B → Approve / Review

1: Reject

2: Reject

3: Review EDD

4: Reject

The Fast Track Known User 2FA

Here you're fast tracking known, good users. Good, trustworthy users are digital identities you can historically (and perhaps heuristically) prove that are good. The most important step is to ensure that the user presenting the data is the user you already trust. You may question how much you would know about a user that you're onboarding for the first time. However:

- You may have a known customer base that you want to cross-sell new services to.
- You may want to transition customers to a higher-level product or service with different capabilities.

In either case, to fast track the onboarding you need to establish that it is the same user and to do that you need two items:

- Criteria to define a good user. This implies some form of historical analysis.
- An identity validation mechanism. The most common tool would be two factor authentication (2FA) through SMS, email, etc... In some instances, device fingerprint can be a reasonable proxy and a substitute for a more strict 2FA mechanism. Device fingerprint is basically frictionless, but should be limited to low-to-mid risk scenarios.

Known User Use Existing Data to Verify the Identity

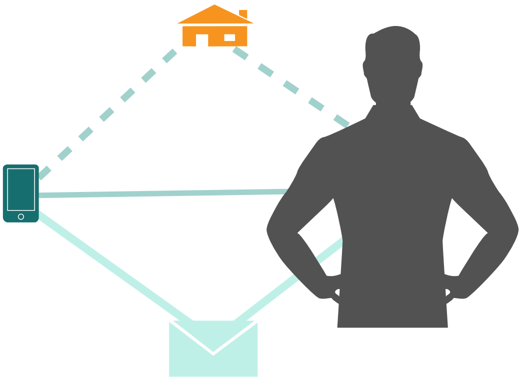
- Previous successful onboarding
- Number of positive transactions
- Frequent transactions
- Recent transactions
- Customer longevity

2FA Ensure the Existing Costumer and New Applicant are the Same Person

- Validate based on device fingerprint. If you have one based ont he stored record, compare it.
- Perform SMS verification. Based on the mobile number on record.
- Perform email verification. Based on the email on record.
- Challenge based on previously set security questions.

If the potential customer is possibly a known good user, you can perform 2FA letting that user select which method they prefer, as those who get to choose are less likely to abandon signing-up. If they fail 2FA, it is recommended to move them through a subset of the rest of the tests (Starting with step 1A). While this might be a simple mistake from the user's perspective, it may also indicate an account takeover. The most important consideration at this point is not to reject them without further review.

1. Is The Identity Real? 1A 1B



Here you're confirming that the applicant's data is consistent, and belongs to a real person. Where the identity information appears legitimate, but there isn't a verifiable correlation between them, you'll want to further validate to ensure they're not synthetic identities. Depending on which country you are operating, and the business application, you may have regulatory requirements to validate the user. You also want to ensure you are dealing with a human, and not a computer.

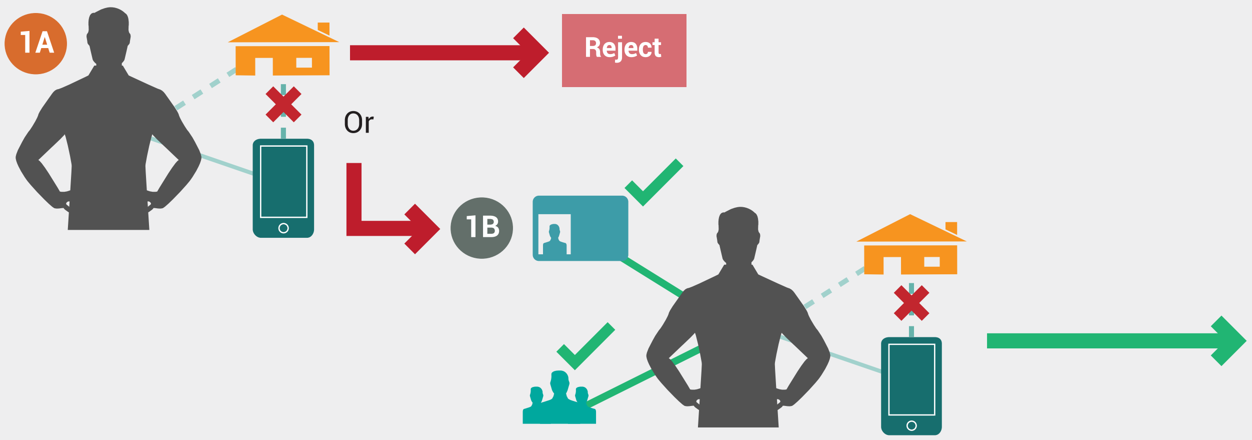
1A Tests to Verify an Identity

- Name to phone to physical address
- Email address to name
- Name to Date of Birth
- Is it a human?

1B Additional Tests

- SSN to name
- Individual is not deceased
- Document Validation: Government issued IDs
- Social network analysis

You may reject any user that fails any of the items in item 1A, however most of our clients choose to run additional tests as sometimes the absence of verifiable data may just be indicative of young users, foreign nationals, individuals who have recently moved, etc. Moving them to a more stringent process (1B) typically includes asking for government issued documents, to verify the documents' validity, and that the data contained in the document is consistent with the data presented. You may find that the identity merits further evaluation despite having failed one test.



However, when you can verify that the information provided is for different users e.g. the phone belongs to one user, the address to another user, and so on, that particular Digital identity should be rejected, and potentially blacklisted so that any aspect of that users digital identity will be rejected from returning.

2. Is the Applicant the Owner of The Identity (or Authorized to Use It)? 2A 2B

Here you're ensuring the identity data is presented by an authorized user. The person trying to onboard may not be the actual user, and in that situation you have to make certain that whomever it is, is authorized to use the information presented. Think of people aiding their elderly parents, or parents aiding their children, or a person that is legally authorized to act on behalf of another person.

The goal is to eliminate the use of stolen identities when onboarding. Data compromises are now commonplace and, as a result, financial services firms must prevent users trying to onboard using stolen identities which appear to be good digital identities. Here are some ways to validate that the potential customer is the person they're claiming to be.

2A Tests to Verify Data Ownership

- Knowledge base authentication (KBA)
- Bank account micro deposits
- SMS response

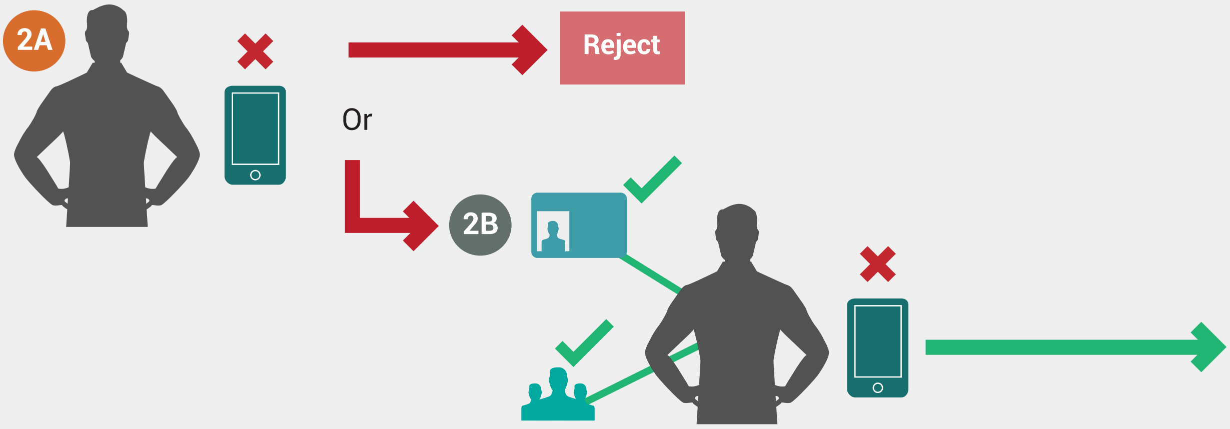
2B Additional Tests

- Document validation: Government issued IDs, utility or cellphone bill.
- Identity data isn't found for sale on dark web
- Social network analysis

On average, about 60% of a user's data has been compromised, and most of this data is available for purchase in the dark web. If data is available it doesn't mean the applicant has done anything wrong, however they are of slightly higher risk.

You may reject any user that fails any of the tests in 2A, however some of our clients choose to run the most stringent tests, detailed in 2B. A potential customer who fails tests in multiple sections such as1A and 1B or 2A and 2B is higher risk than one who fails in just one, and at the very least should be considered very high risk.

For potential customers that pass all of the tests, you still need to answer a couple of more questions.



3. Regulatory Requirements: Can You Do Business With The Identity? 3A 3B

Although you may have incorporated some regulatory requirements in the previous sections, this is where regulation applies more directly. Certain regulations have specific requirements you need to fulfill. For example, your business may not be authorized to service users in certain countries, or only operate in certain states, or users may need to be a certain age, etc.

Which tests you need to perform depend on which country you operate in, and what regulations your business is subject to.

In most cases, the requirements associated with identity data include: location, age/date of birth, and sanctions.

Location

Defining location can be tricky. You have to consider billing and shipping address, IP address geolocation, where payment instruments were issued, where transfer of money is going into, phone area code, government id issuance, and perhaps more. Users may attempt to trick you with one of the locations above, so knowing what combination is allowed is fundamental to develop an automated program.

Date of Birth

Notably financial services, gambling, online gaming, and dating, to name few businesses, require users to be of certain age. Minors trying to access adult websites, online gaming, dating and gambling is a very common situation. Minors will try to impersonate their parents. This situation can be difficult to spot without some form of friction. Tests in this section combined with those of the authority of use identity data are very important.

Sanctions

Every financial transaction in the US has to be screened against various sanctions lists. Sanctions lists contain the name of users and businesses, sometimes even whole countries, that you can't do business with. Almost every country has sanctions lists that Financial Service firms need to abide by. In the United States, these are published and maintained by OFAC. In Canada by FinTrac, and so on.

If you happen to be offering financial services, you are likely required to screen your potential users against a PEP (Politically Exposed Person) list, both at onboarding and then periodically. PEPs are public figures that are at higher risk of bribery or corruption. The risk of a PEP depends on their public position. For example, the President of a country has a different risk level than the Mayor of a small town.

3A Tests to Screen for Regulatory Requirements

Location

- Shipping/ billing address
- IP geolocation
- Phone area code

Age

- SSN to Date of Birth
- Name to Date of Birth

Sanctions

- Name match
- Date of Birth match
- Address match
- Public position

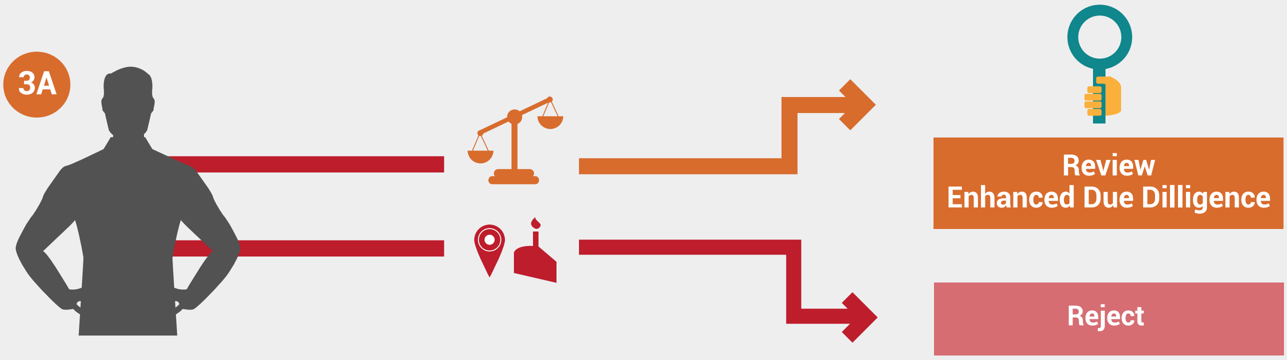
3B Additional Tests

- Document verification
- Bank account micro deposit
- Knowledge based authentication
- Enhanced due diligence
- Negative news

A potential user or business that matches against sanctions or PEP lists has to be manually evaluated. There is an operational burden to vet identity matches against sanctions and PEP lists, as the matching algorithms against these lists are usually tuned liberally, meaning they match more than they should. This is to minimize missing an individual or a business that could be part of a country's sanction list.

While the operational burden is high, you can estimate that in general 5% - 10% of your clients will match against one of these lists.

Users that fail location or Date of Birth tests usually end up being rejected.



4. Online Risk: What is the Risk Posed by The Identity? 4A 4B

By now, you probably have a pretty good idea of the quality of the identity data presented, and in all likelihood, assuming positive results, you are likely dealing with the right person, which will turn out to be a good customer. However, for those of us in the business of providing services to detect online fraud, we have to look at the environment and the risk models that apply to your business as well.

In this area you'll want to measure the risk that the user may pose to you. The type of things you need to look at are varied and touch multiple dimensions.

Affiliation and Affinity

An individual or a business that is associated with nefarious organizations can be problematic to your reputation. The funding of terrorism, unfortunately, usually involves "good" individuals and businesses that are hard to detect.

Data Link Analysis

The overall relationship of the identity data. For example, a user is likely to have only one account, so if identity data is correlated across multiple accounts, it is likely suspicious. Especially if these attributes show some form of velocity.

Location Analysis

Inconsistencies in location pointers: IP Geolocation, vs billing address, vs government issued ID location, and so on.

Device Risk Signals

Analysis on the actual device looking for malware, jail broken, cell phone burners, etc.

Payment Analysis

Look for signals of chargebacks, ACH refunds, and credits. These are early indicators of risky user behavior.

4A Tests to Evaluate Risk

- Number of connections of identity data
- Device compromise
- Location irregularities
- Velocity
- Chargebacks and Credits

4B Additional Tests

- Affinity to known nefarious individuals/organizations

The intrinsic nature of risk analysis tends to highlight a large set of indicators, and one can get lost into the signals if not careful. Experienced risk analysts will quickly recognize the level of scrutiny that a business can tolerate and develop policies that are adequate to the business itself. Business owners should work in conjunction with risk and compliance to achieve a balance between all these competing requirements.

Conclusion

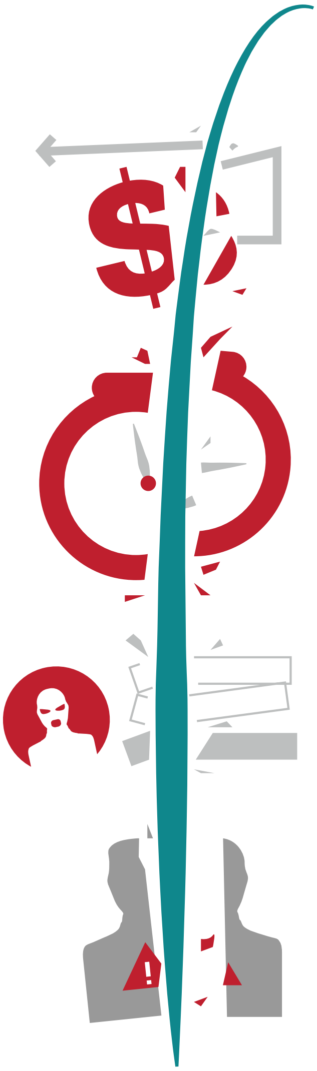
Globalization and the ability to offer financial services online has great benefits for businesses that can take advantage. To add customers, you need a strategy that includes regulatory requirements by country, risk analysis for online transactions and behavior, and more importantly: user experience. This is a shared strategy across the company stakeholders, and it would be in your best interest in making sure no single component dominates the strategy.

Technology has advanced to help businesses achieve a balance, minimize the risk and comply with ever changing regulations while still enabling achieving their goals. Savvy compliance officers and risk analysts will know how to best make use of technology and tools. User experience managers should also take advantage of the business model to ask customers for the needed information and turn such information into customer base insight that can be used for better applications.

The concept of Digital Identities is sound and provides a clear framework on how to think and traverse all these fields. We must not forget we are dealing with users and the best way to analyze risk and assure compliance is to model the risk strategy as close as to what they are. The best decisions are made when there is enough information about the users and their intent.

Trusted Digital Identities in Action

The IDM platform provides a much needed Digital Identity Layer to Financial Services. Leveraging an API, this layer powers the usage of identities 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:

Reduction of Transactional Fraud

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

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%.**

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.

Reduction of False Positives in Sanctions Screening

Our platform offers many ways to reduce false positives and to tune the matching algorithms. The eDNA^{TM} information of both the identities evaluated and those in sanctions and PEP lists allows for multi-attribute comparison.

Want to use Digital Identities to Increase Your Efficiency?

We pioneered the use of Digital Identities in fraud prevention and compliance, and we'd be glad to to show you how 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 95%, 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 is updated in real time, with data from our extensive customer base covering multiple industries: banks, money service businesses, virtual currencies, online lending, payment service providers, ecommerce merchants and fintech.
- Visual analysis. Explore our eDNA™ technology in detail, and see how we visually correlate multiple parameters for every user identity with our Entity Graph.

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

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