Synapse

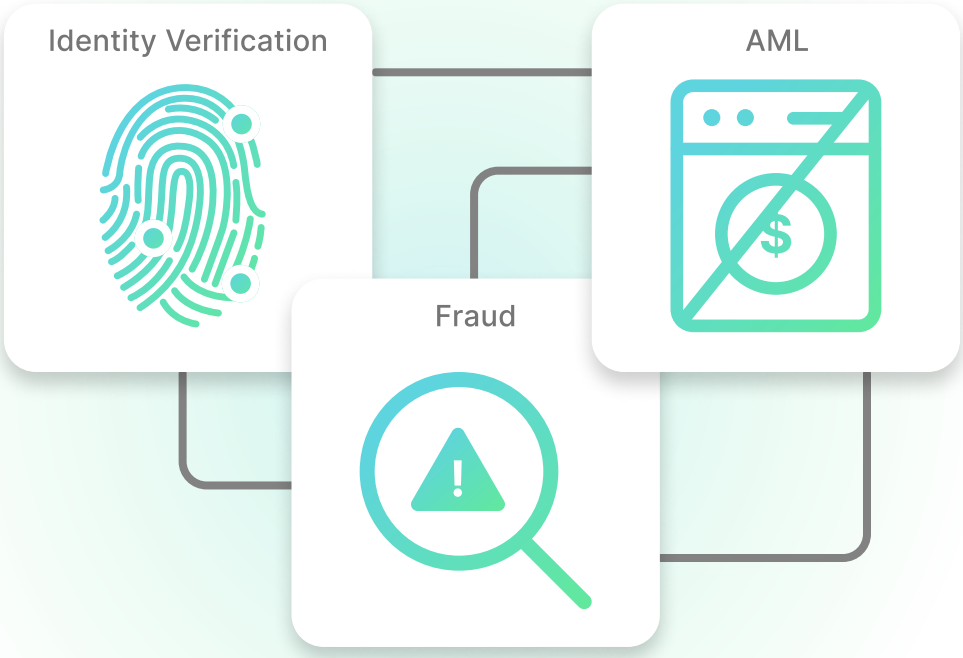
A Modern Trust Framework for Identity Verification with a Look to the Future

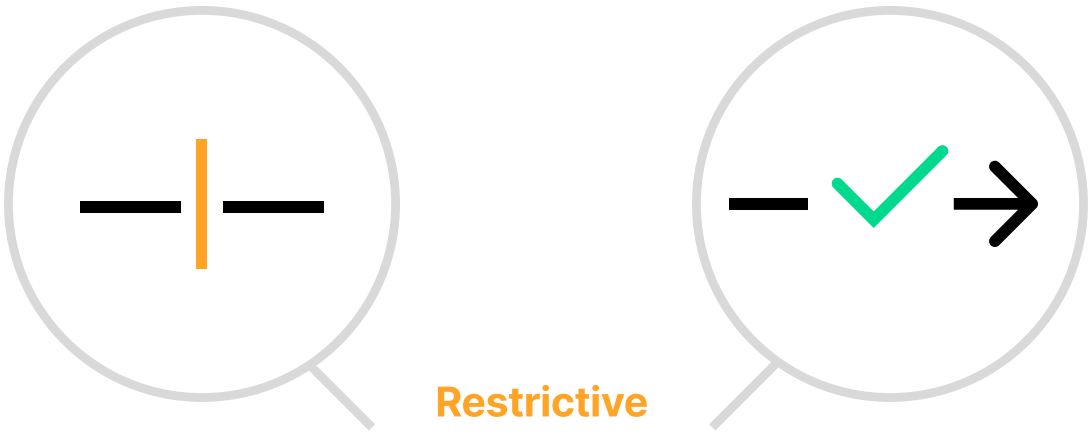
Contents

Fintechs invest significant resources to protect themselves and their users against identity theft, fraud, and money laundering schemes. Yet the number and the variety of those schemes are growing rapidly.

- According to the **FTC**, U.S. consumers reported losing more than $5.8 billion to fraud in 2021, a 70 percent increase over the previous year.
- The number of identity thefts reported to the **FTC** in the U.S. in 2021 was nearly 1.7 million.
- According to **Javelin Strategy & Research**, identity theft cases in the U.S. resulted in losses of $56 billion in 2021, a 79% increase from 2020.

In this Thought Guide, we will explore the strategies fintechs are deploying to get ahead and stay ahead of these schemes and still deliver great experiences for their users. If you're an executive, a senior engineer, a product manager, or another fintech innovation decision-maker, this Thought Guide is for you. It will outline a modern vision of identity verification and paint a vision of the future.





Restrictive

or

Permissive?

What approach to identity verification is right for my platform?

For every fintech and **embedded finance** company, getting the information they need for accurate identity verification without losing the potential user is a challenge. Fraudsters and legitimate users gravitate toward platforms with the least friction for identity verification, so there is no single model that dissuades only bad actors. Platforms want to onboard as many users as possible, but depending on the operating principles of their identity verification, the platform may see significant onboarding abandonment rates. The more information the platform asks of the potential user early in the onboarding process, the higher the abandonment rate.

Creating an initially high requirement for identity verification may be a necessary evil. For example, high-volume or high-value transactors where a single transaction or multiple transactions in a short time could, if fraudulent, materially injure your balance sheet or profits. This type of high initial identity verification is characterized as a **Restrictive Model.**

Restrictive Identity Verification Model

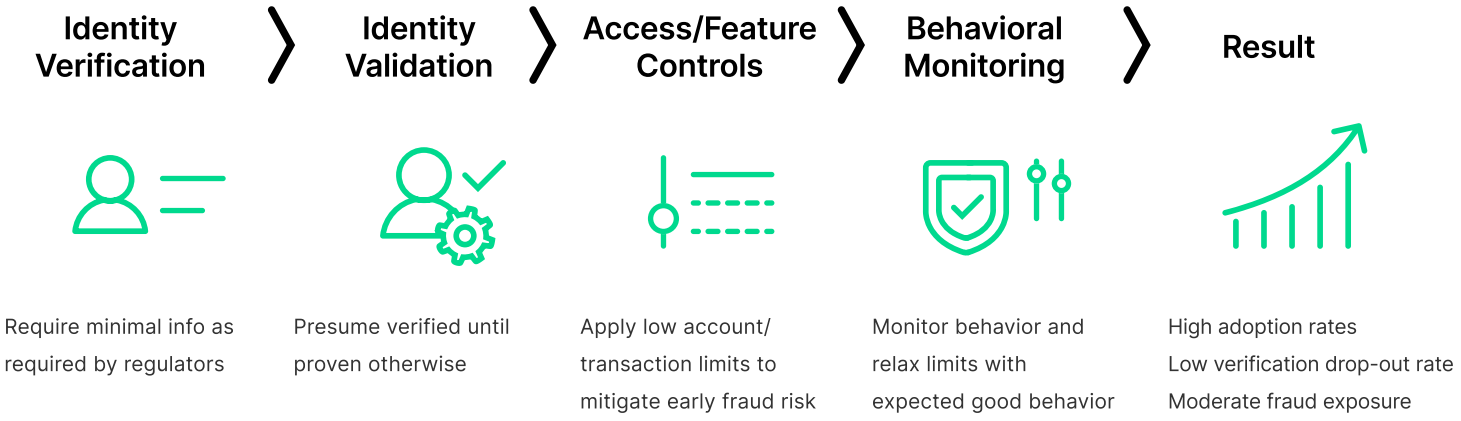
With a restrictive model, the platform asks for as much information up-front as possible to meet all regulatory requirements as well as minimize fraud risk. One effective approach to limiting financial exposure to fraud is to limit the frequency and value of transactions, at least until further verifications can be completed. However, if your users are high net-worth individuals for which $10,000 transactions are commonplace, your platform will not get away with limiting their traction value to $500 until additional verification checks can be completed. Any transaction restrictions at levels too low to be effective for this type of user would render your service essentially unusable, and they will defect immediately. Because of the scale of financial risk, even your initial transaction values or volumes will necessarily be at a relatively high level to be effective for this user audience. Complete identity verification will be required upfront, lest you expose your platform to extreme losses caused by bad actors that will undoubtedly slip in, exploit the vulnerability, and move on.

Identity Verification	Identity Validation	Access/Feature Controls	Behavioral Monitoring	Result
				
Require all info required to minimize platform fraud risk plus that required by regulators	Presume unverified until proven otherwise	Enable high account/ transaction limits from the outset	Monitor behavior and decrease limits with unexpected bad behavior	Low adoption rates High initial verification drop-out rate Minimal fraud exposure

Alternatively, if your user base is more like everyday consumers, you have an alternative identity verification option, specifically the **Permissive Identity Verification Model.**

Permissive Identity Verification Model

In this model, the platform asks the least amount of identity verification questions during the initial account creation step, based on the bare minimum of what regulators require. In this approach, identity verification steps are spread between initial account setup and downstream account engagement. With increasing trust established over multiple steps, users are granted increasing transaction value and volume authority. This strategy also depends on establishing low, medium, and high transactional thresholds based on the trust level achieved over time. For example, upon initial account setup, users may be limited to $500 per day in transactions until downstream verifications can be completed, then increased to $5,000 per day. The other key benefit of Permissive Identity Verification is that a platform can augment identity verification with passive behavioral analytics and indirect social vetting. This makes it possible to develop a rich assessment of identity without an explicit request for extensive documentation. From a user perspective, this model can feel extremely light on onboarding friction, welcoming the user journey. Light onboarding friction could lead to greater customer loyalty, longer lifetime value, and higher long-term profitability for your platform.



> "It's really hard to build a delightful, frictionless experience and, at the same time, be maniacal about protecting our users and ourselves. It's such a delicate balancing act."
>
> Hrishi Dixit, CTO, Yieldstreet

Yieldstreet is reimagining the way wealth is created by providing access to alternative investments previously reserved only for institutions and the ultra-wealthy. Yieldstreet's mission is to help millions of people generate $3 billion of income outside the traditional public markets by 2025. Its award-winning technology platform provides access to investment products across a range of asset classes such as Real Estate, Commercial, Consumer, Art, Marine, Legal Finance and Aviation. Since its founding in 2015, Yieldstreet has funded over $1.9 billion of investments and is committed to making financial products more inclusive by creating a modern investment portfolio. The company, headquartered in New York City with offices in Brazil, Greece, and Malta, is backed by leading venture capital firms. Yieldstreet is a Synapse customer.

Should identity verification happen once or be an ongoing process?

Today, identity verification, or know your customer (KYC), is a point-in-time event. The identity is confirmed, and the platform either authorizes the customer as a safe user, or they don't. But should identity verification be a point-in-time event? Should we continue the identity verification process beyond the initial sign-up phase because people and things change? For example, a user deemed trustworthy during onboarding could fall victim to identity theft, and that person could be conducting fraud. Unless the platform performed subsequent identity verification processes, they would not know the fraudulent activity was occurring.

There is merit in a verification strategy that promotes continuous trust verification with users. Platforms can interpret KYC as two halves of one whole:

- Are you who you say you are?
- Are you still the same person we authorized earlier?

> "Maybe the two problems are initial trust and ongoing trust, and ongoing trust encompasses fraud but other vectors as well."
>
> Sankaet Pathak, CEO, Synapse

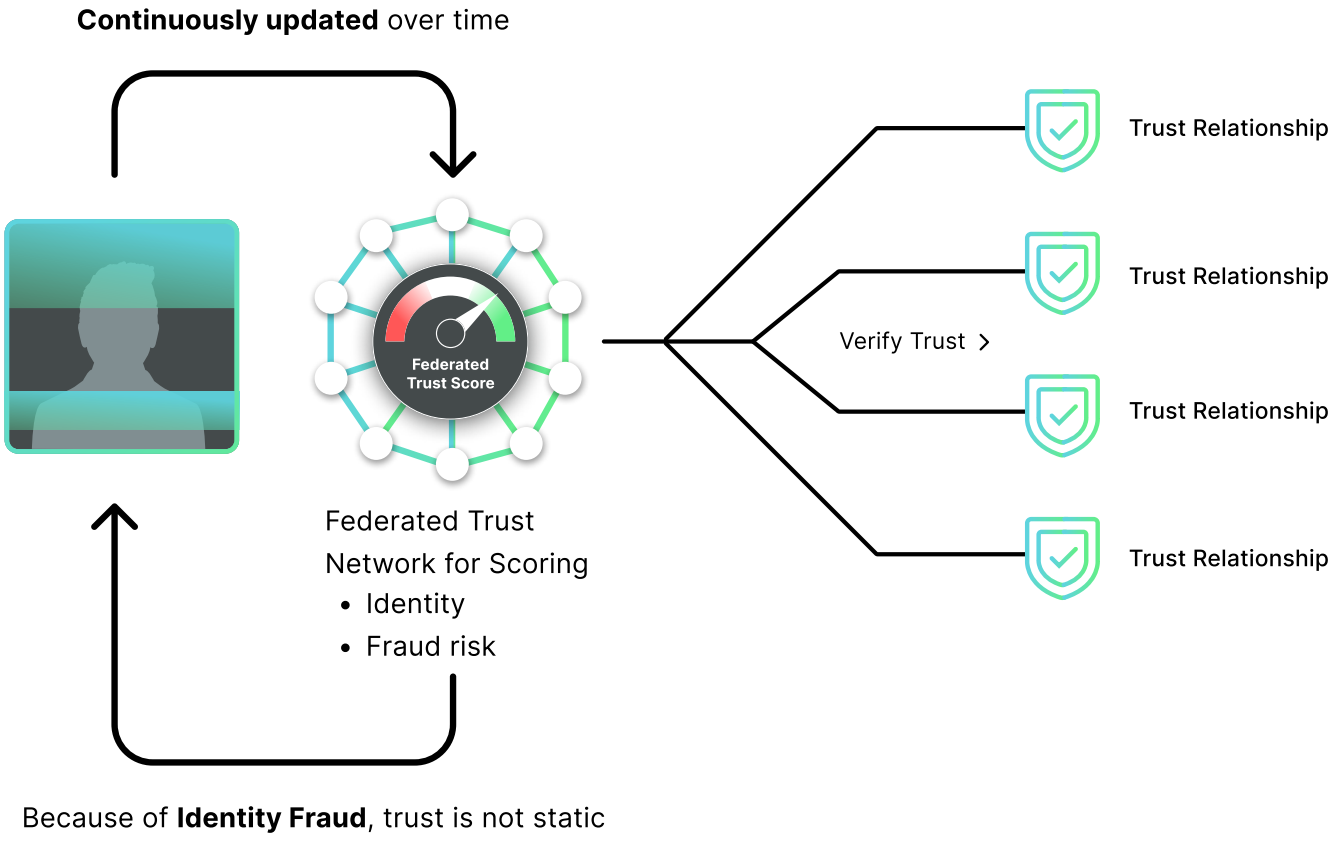
What could the future of identity verification look like?

Technologists looking for a way to scale quickly are starting to envision an architecture that consolidates and stores consumer verification information and formulates this into ID scores. Platforms can access the ID scores to inform their authorization processes, and users can designate the information they share with each platform. It's faster for the platforms and convenient for users who don't have to input the same identity information repeatedly.

Synapse's ID Score is a possible precursor to this type of identity verification process. ID Score assesses the likelihood that the identity supplied belongs to the person who is creating the account. ID score outputs three risk levels: low, moderate, and high, based on identity documentation and millions of fintech transactions. The fintech gains value by adjusting risk management according to the fintech's risk appetite. For example, a user with a high level of risk could be restricted to transacting 10% of the daily limit on the platform relative to the limits of a user with a low-risk score. ID Score also monitors transaction decisioning with explainable reasons why a transaction was blocked. ID Score is improving the KPIs of fintechs by allowing faster user onboarding with reduced loss rates and fraud user detection.

But what if, when a user joined a new financial service platform, they did not have to restart from a trust level of zero? What if the new platform could reference the user's trust level or ID score from another platform that has a long history with that user? Wouldn't that be amazing for that user? The concept could be implemented from a BaaS platform quite easily if the two fintech platforms were built on the same BaaS platform, such as Synapse. The user's Synapse ID Score could follow them from old to new service providers.

Now take this concept and extend it to fintech services built on unrelated platforms. Imagine if Synapse and other core **BaaS platform providers** agreed to a protocol for sharing ID scores in a secure manner externally. Now, you have Federated Identity, where a user's trust level for identity would follow them from platform to platform. Now imagine through big data, a massive amount of identity data is collected and scored, and the platforms subscribing to this data are global. Then you will have a Global Federated Identity. Naturally, this network would require a consortium of data providers and a very safe, highly encrypted environment that could share data across multiple SaaS platforms. That said, this could represent the future of identity verification and user trust level portability.



"...the vision is to make onboarding into a financial ecosystem as simple as that of a social network with federated identity."

Sankaet Pathak, CEO, Synapse

Where does trust fit into the identity landscape?

Whether or not we can trust one another is at the core of identity, fraud, and AML, so why isn't trust at the center of the discipline? Mainly because we've put identity and fraud in front of trust. When a platform is onboarding users, they go through a series of identity verifications to determine if they are onboarding the right person they deem safe or trustworthy.

As the relationship continues, the platform conducts several trials to ensure a low chance of fraud and to determine the trustworthiness of that customer at that point in time. So trust is the goal of the identity, fraud, and AML efforts, to know enough about the person to feel comfortable trusting them or not trusting them on the platform.

Can trust be transitive?

Do trustworthy individuals usually associate themselves with other trustworthy individuals? What types of relationships have the strongest implications for trust parity? These are the fundamental questions upon which any transitive nature of trust would be based.

There is precedence for the transitive nature of trust. Job interviews, college applications or loan applications, requests for references, or contacts that can vouch for you, are effectively based on the belief in transitive trust. They believe that if trustworthy people vouch for you, then some of that trust transfers to you.

Other factors come into play, such as the length of time and consistency of relationships, the number of trust relationships you have over time, and the credibility and independent trustworthiness of the referring party.

So it holds that trust is transitive, and therefore leveraging a federated network of trust scores (in addition to the relationship between related parties and their trust scores) could be a valuable source of trust scoring. Trust scoring could accelerate access to services, even in new service platform relationships, benefiting users and platforms alike.

Leveraging the scalable advantages of the Federated Trust, over time, it could be possible to extend the trust levels of individuals and related parties and have that trust level follow them to new platform relationships. For example, suppose the Federated Trust network trusts a person who was employed at a company for five years; they will likely trust a colleague who worked directly with that person for those five years, even if they bank at different institutions or use different financial services platforms.

The practice is already at play in many marketplaces today. Companies like Ebay vet their merchants and sellers based on their LinkedIn and other social profiles. Apple and Lyft check the time and tenure on major social media platforms like Facebook, LinkedIn, and Twitter to corroborate other data. They are using relationship vetting to conduct a version of transitive trust.

If you're interested in learning more about modern identity verification, we welcome you to listen to the Under the Hood podcast, season 2.

> "If someone who's previously verified and deemed as good suddenly turns out to be bad, nine cases out of 10, it's going to be because of the actual identity being stolen."
>
> Hrishi Dixit, CTO, Yieldstreet

About Synapse

Synapse empowers companies of all sizes and across all industries to become innovative financial partners for their customers. We are the largest Banking-as-a-Service provider that enables builders to launch feature-complete deposit, credit, and crypto products in weeks.

With Synapse's APIs, companies can design products and services that raise access to financial services for all. We help builders develop and launch custom suites of financial services to embed banking products, issue cards, provide next-generation loans, crypto products, and more, quickly, reliably, and securely.