Trulioo | GLOBALGATEWAY®

The digital identity network

A holistic approach to managing risk in a global economy

Table of contents

Introduction

The struggle to build trust online

For a digital economy to thrive, there has to be trust online. This trust provides the assurance that global businesses need in order to securely offer goods and services to customers, whether that's through financial transactions, shopping, exchanging services, or gaming and entertainment.

This paper:

- Discusses the challenges global businesses have with identity
- Examines the limitations of traditional identity solutions
- Describes how a digital identity network enables a risk-based approach to identity challenges
- Provides use cases for how a digital identity network enables participation in the global digital economy

Digital identity is the catalyst for establishing trust, and verifying digital identity as part of the onboarding process is the first step toward building that trust. Digital identity verification affirms that the customer is who they say they are. With this assurance in place, a company can confidently allow the customer to begin transacting online.

Identity verification during onboarding is just the start, though. As customers engage in higher-risk or higher-value transactions, businesses should correspondingly increase the level of assurance by adding layers of verification and authentication. While they may only use a basic Know Your Customer (KYC) check during account creation, businesses need additional verification checks before approving loan applications or high-dollar purchases, for example.

These different use cases, along with each customer's unique set of identity attributes and risk profiles, creates immense complexity for global businesses. To maintain online trust in such a diverse environment, businesses in the digital economy must incorporate adaptable and robust methods for identity verification. All too often, however, digital identity verification is an inefficient, risk-prone process that does anything but build trust.

Analyst firm Deloitte calls customer identification the "linchpin of online transactions," stating that "the need for a digital solution is becoming urgent. Transactions are growing in volume and complexity. Customers increasingly expect seamless, omni-channel service delivery and will take their business elsewhere if they don't get it. Regulators, for their part, are demanding greater insight into transactions. They'll hold firms responsible if identity information is missing or inaccurate. Finally, the sophistication of digital attacks is rising. Hackers can exploit weak identity systems more readily than ever, wreaking financial and reputational havoc in the blink of an eye."[1]

The problem is the internet — it lacks a critical identity layer that would solve the complex problems Deloitte talks about. While there are layers of protocols and methodologies for transporting data over networks, there is no protocol for transporting assurance. In online transactions, then, there is no standardized way to establish that an individual is who they say they are — the essence of identity.

Without this assurance, businesses struggle to build trust online. Identity companies have created countless solutions to establish trust, from basic data verification to sophisticated biometric authentication. Individually, these solutions fail to solve the internet's fundamental problems with identity. They lack the robustness and flexibility to battle evolving fraud, comply with multiplying regulations, meet increasing demands for a seamless user experience and provide accessible digital services.

To keep pace in the fast-changing digital economy, we need to reimagine identity — look at both the problems and solutions in a new, more holistic way. In other words, we need to create that missing identity layer.

[1] Deloitte Touche Tohmatsu Limited, *Picture perfect: A blueprint for digital identity*, 2016.

Risky business

Global companies battle fraud, compliance and digital access across borders

Without the ability to establish trust online, companies face significant barriers to expanding their business in the digital economy — especially on a global scale.

These challenges include preventing fraud, complying with a bewildering patchwork of regulations and ensuring digital access to customers around the world.

Fraud

Cybercriminals are clever and ambitious, perpetrating increasing amounts of fraud. In the U.S., new account fraud was up 13 percent in 2018,[2] and mobile phone account takeovers skyrocketed 79 percent that same year.[3] Globally, money laundering is estimated at 2 to 5 percent of global GDP,[4] while cybercrime is expected to reach a cost of $6 trillion annually, starting in 2021.[5]

[2] Rob Douglas, *ConsumerAffairs*, "2020 Identity Theft Statistics," May 14, 2020.

[3] Kyle Marchini, Al Pascual, Javelin Strategy & Research, "2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt," March 6, 2019.

[4] United Nations, "Money-Laundering and Globalization," March 2020.

[5] Steve Morgan, *Cybersecurity Ventures*, "2019 Official Annual Cybercrime Report," March 2020.

Regulatory compliance

Concerned lawmakers are cracking down on fraud, money laundering and identity theft with an upsurge in regulations, including Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements. Fines for non-compliance are stiff; in 2019, 58 AML penalties totaled more than $8 billion in fines globally.[6] More recently, an Israeli bank was fined nearly $1 billion for tax evasion and anti-money laundering.[7] And in the U.S., financial institutions have been charged nearly $24 billion in fines since 2008.[8]

Making sense of the dozens — or even hundreds — of regulations is a challenge, as is ensuring compliance. There are an average of 220 regulatory alerts per day,[9] and the volume of regulatory changes and announcements increased 492 percent since the 2008-09 global financial crisis.[10] The concept of RegTech did not even exist 10 years ago, but by 2020 it was expected to consume 34 percent — $76 billion — of all regulatory spending.[11]

In the U.S., financial institutions have been charged nearly **$24 billion** in fines since 2008.

[6] Brian Monroe, Association of Certified Financial Crime Specialists, "Fincrime Briefing: AML fines in 2019 breach $8 billion, Treasury official pleads guilty to leaking, 2020 crypto compliance outlook, and more," January 14, 2020.

[7] Steve Hendrix, *The Washington Post*, "Israeli bank fined nearly $1 billion in U.S. tax evasion, money laundering cases," May 1, 2020.

[8] Rupert Chamberlain, Jim McAveeney, Chetan Nair, Andrew Husband, Richard Robinson, KPMG, "Combating financial crime," March 2019.

[9] Susannah Hammond, Stacey English, Thomson Reuters, "Regulatory Intelligence Cost of Compliance Report," 2019.

[10] Iwona Tokc-Wilde, ACCA Global, "Regtech to the rescue," March 1, 2017.

[11] KPMG, "There's a revolution coming: Embracing the challenge of RegTech 3.0," 2018.

Digital access

A large fraction of the world's population struggles with accessibility to core digital services such as banking. In emerging economies, 2 billion individuals and 200 million micro, small, and midsize businesses don't have access to savings and credit,[12] and those with access usually pay high fees for a limited product selection.

Even consumers in established economies lack access. More than 25 percent of U.S. households are unbanked or underbanked, meaning they have a checking or savings account and also use products or services from an alternative financial services provider, such as money orders, check cashing or payday loans.[13] To access their own money, unbanked Americans spend nearly $500 annually — 15 times what people with full access to banking services pay in fees.[14]

[12] James Manyika, Susan Lund, Marc Singer, Olivia White, and Chris Berry, McKinsey Global Institute, "How digital finance could boost growth in emerging economies," September 21, 2016.

[13] Gerald Apaam, Susan Burhouse, Karyen Chu, Keith Ernst, Kathryn Fritzdixon, Ryan Goodstein, Alicia Lloro, Charles Opoku, Yazmin Osaki, Dhruv Sharma, Jeffrey Weinstein, FDIC, "2017 National Survey of Unbanked and Underbanked Households," October 2018.

[14] Jason Miles Lorimer, *Medium*, "Unbanked: How Alternative Financial Services Are Strangling American Families," April 6, 2017.

Peeling back the layers

The challenges of traditional identity solutions

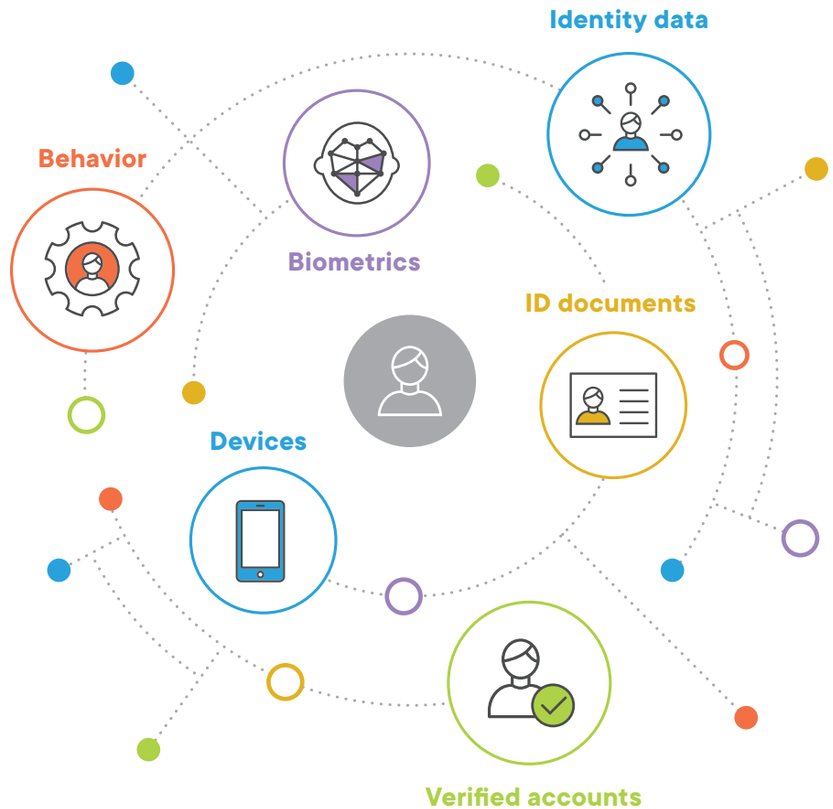
These problems are difficult to solve because the attributes that make up identity are always shifting.

We can consider identity as a mosaic of unique attributes that change as we change, such as when we move, change our name, get a new job or open a new line of credit. Therefore, establishing identity is a moving target, and the processes for creating assurance, such as authentication and verification, must adjust accordingly.

As much as identity evolves, however, one thing never changes: prioritizing privacy and security while creating a frictionless user experience. Consumers want to know their information is safe and secure, but they also want to be "remembered," so they don't have to be validated every time they interact with an online entity.

A recent study found that 62 percent of U.S. and UK customers value "security over speed" when it comes to account creation.[15] Yet people won't tolerate pointless friction, either. The same study revealed 42 percent of consumers will abandon the account creation process if the service provider fails to verify their identity after multiple attempts.

To maintain this balance while addressing the problems of fraud, compliance and digital access, businesses should take a network approach to identity. **A digital identity network leverages hundreds of data sources and technologies to satisfy these challenges and create the seamless experience users have come to expect.** A digital identity network also helps fill the gap created by the internet's missing identity layer.



[15] Trulioo/Insight Avenue, *Consumer Account Opening Report 2020: The Power of First Impressions Online*, 2020.

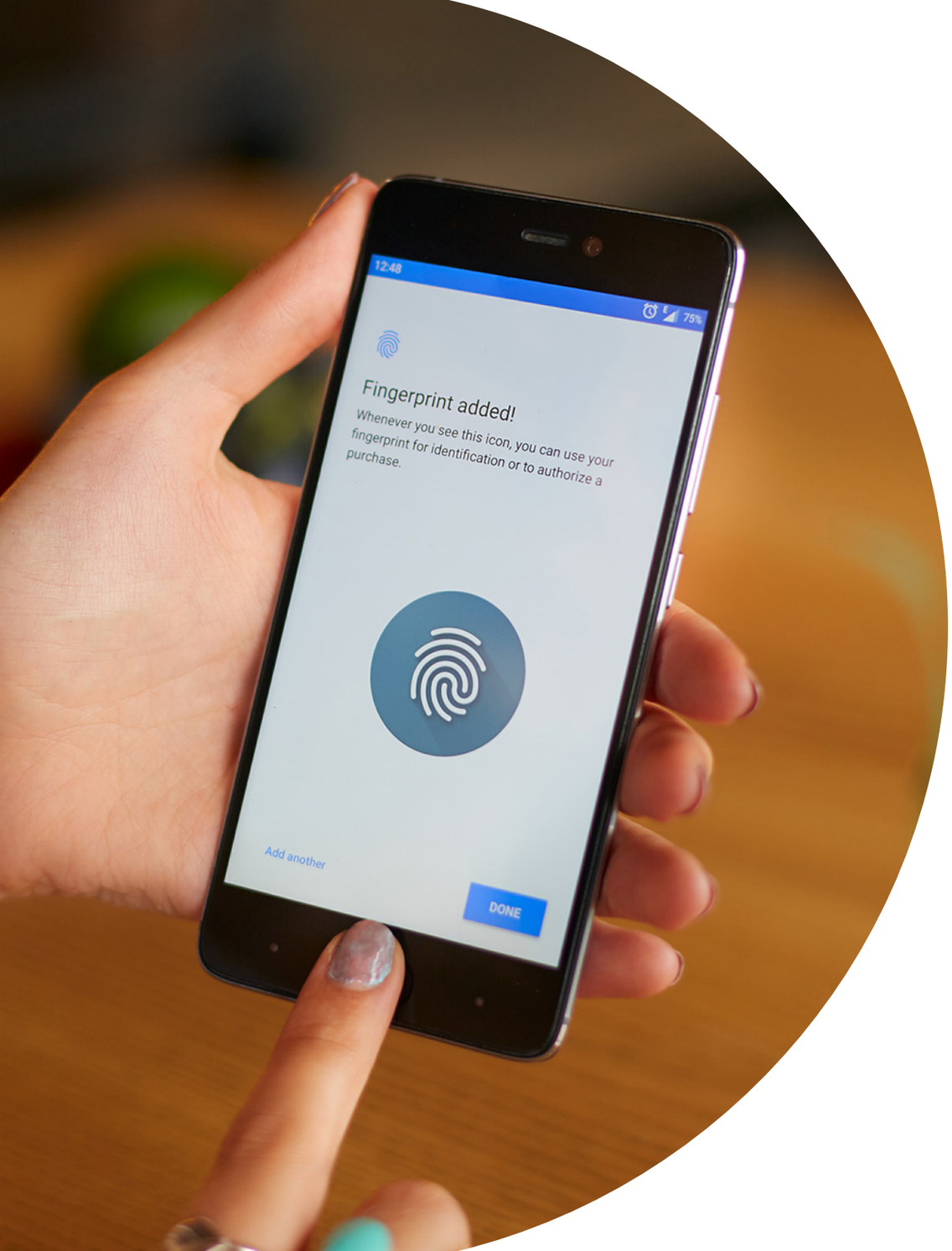
However, today's identity solutions are often incomplete and lack the depth of capabilities required to form this network of data sources and technologies. The analysts at Deloitte take a multilayered look at the barriers to "building a full-fledged identity solution that could be put into broad commercial use"[16] (see Table 1).

The Deloitte report further points out: "Many efforts today address one layer but not others. For instance, authentication technology solutions tend to rely on attributes that have already been collected. These solutions provide a better experience for users and ensure that the same person is transacting each time, but it doesn't help identify who that person really is."

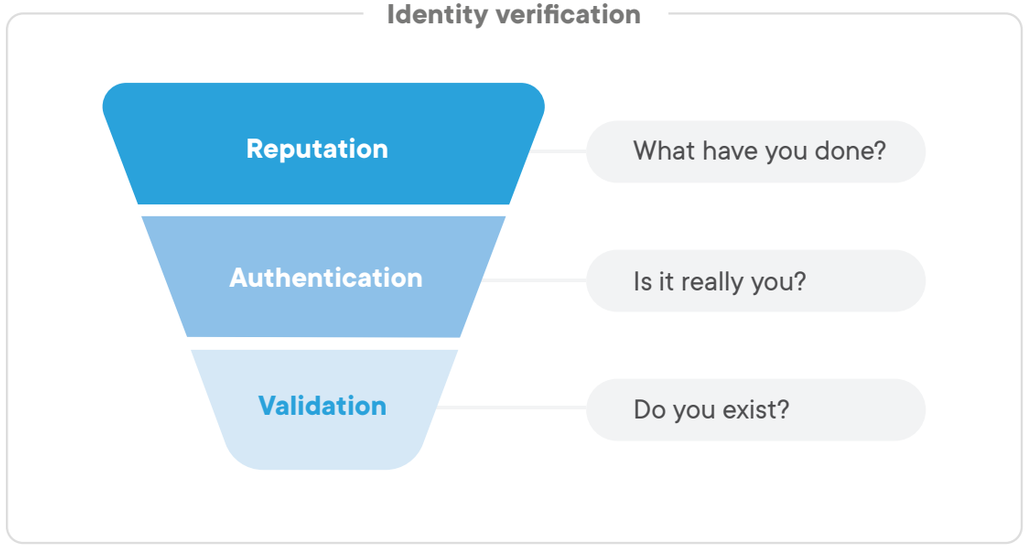
Table 1. Challenges of different identity layers

Identity Layer	Purpose	Problems
Service delivery	Offer seamless services to users	Inefficient or unsuited delivery
Authorization	Provide the services to which users are entitled based on their attributes	Complex authorization rules and relationships
Attribute exchange	Provide ways to exchange attributes between parties	Lack of security and compromises to privacy
Authentication	Provide ways to link users to attributes	Weak or inconvenient authentication
Attribute collection	Capture and store user attributes	Inaccurate or insufficient attribute collection
Standards	Develop standards to govern system operation	Lack of coordination and consistency

[16] Deloitte Touche Tohmatsu Limited, *Picture perfect: A blueprint for digital identity*, 2016.



These technologies focus on the method for establishing identity rather than solving the problem, which is creating the proper level of assurance needed for both businesses and consumers to confidently participate in the digital economy. Take Deloitte's example of authentication methods that rely on existing attributes. It doesn't answer all the questions needed to fully assess the risk of a specific individual — to create that assurance:



This limited view is further compounded by the mosaic concept of identity discussed earlier. If any of these attributes change — and they often do — does the method selected for assessing risk take this change into account?

Taking a risk-based approach

A look inside the digital identity network

Deloitte researchers call for a way to "tie solutions together so they form a strong identity system. Something that's convenient, effective, lets users control their information and protects their information where it is in use. Something that can handle large transaction volumes and makes good sense for everyone involved."

Similarly, analyst firm Gartner notes the need for tools that enable the orchestration of multiple vendors and capabilities, allowing for frictionless workflows and single unified processes for cross-checking data.[17] This orchestration of processes and data sources helps shift the focus from a particular method for establishing identity to mitigating the evolving risk associated with doing business in the digital economy — such as fraud, compliance, access, security and customer satisfaction.

This risk-based approach provides a holistic view of identity challenges. Viewing them as a whole provides context, so companies can leverage the capabilities of a digital identity network in a way that makes sense for their business. These companies can focus on the strategic rather than the tactical.

To manage risk while accounting for the evolving nature of identity, a digital identity network must be agile, optimized and diversified.

[17] Akif Khan, Jonathan Care, Gartner, "Market Guide for Identity Proofing and Corroboration," September 30, 2019.

Agile

A digital identity network intelligently and swiftly adapts to the business context, which may be determined by many factors, including:

- Location of the business and customers
- Applicable regulations
- Consumer adoption of technology
- Company size and industry
- The purpose of verification or authentication, such as customer onboarding or authorizing payments
- Identity attributes to be verified, authenticated or screened, including personally identifiable information, ID documents, behavior and biometrics

Any change in these factors causes the business context to shift, and the digital identity network adapts accordingly. For example, a business could create custom verification workflows based on each type of customer and transaction. For account creation, the business may only need a KYC check against a few data attributes. For higher risk transactions, the business would want a higher level of assurance against fraud.

To establish that trust and safety, the business could add on layers of verification, such as ID document verification. The more layers used to establish identity, the greater the level of assurance — and therefore a reduced likelihood of impersonation, account takeover or fraud.

Optimized

As the above example illustrates, businesses often require more than one method for establishing identity. The digital identity network needs a centralized function that intelligently deploys the appropriate tools and data sources to arrive at the appropriate decision. An optimized network will dynamically route to the highest-performing data sources and identity services.

Gartner lists three requirements that need to be met for this "orchestration" — or optimization — to be effective:

1. "Integration to multiple tools across the range of capabilities that the organization requires
2. "Ability to design workflows that facilitate applying the different tools and capabilities either in parallel or series, with the ability to apply logic and invoke particular tools only if specified conditions are met
3. "Functionality that enables a single decision to be reached based on the outputs of the various applied services"[18]

Another requirement for optimization is that a digital identity network continually evolves. The provider constantly monitors the network's success and performance, adding new services or tools, incorporating user feedback, and using technology such as artificial intelligence (AI) and fraud scoring to keep current with the latest threats and regulations. This continual evolution ensures the network is optimized for each business based on their use cases, risk exposure and current environment.

> **An optimized network will dynamically route to the highest-performing data sources and identity services.**

[18] Akif Khan, Jonathan Care, Gartner, "Market Guide for Identity Proofing and Corroboration," September 30, 2019.

Diversified

A digital identity network is inclusive, providing access to all the tools, methods and data sources needed to participate in the digital economy — anywhere and everywhere. For example, a customer in North America who wants to open a bank account could easily walk into a branch and have a face-to-face, non-digital experience. Alternatively, they could create an account online with their laptop. The bank could run a KYC check against established identity attributes such as a government ID number, employment information or driver's license. This is easily done because the customer likely has a credit file history or an established relationship with a government organization.

On the other hand, a customer in an underserved market like the Philippines or sub-Saharan Africa might have limited documentation and government services. However, they are likely to have a mobile phone tied to their identity. To provide this customer with access to financial services, a bank would need multiple verification and authentication layers to reach the proper levels of assurance. The business could use the customer's mobile phone to provide:

- Device authentication through a mobile network operator
- Biometric authentication, which compares a selfie photo to the photo on an ID document
- ID document verification, which captures images from a person's ID document and assesses its validity

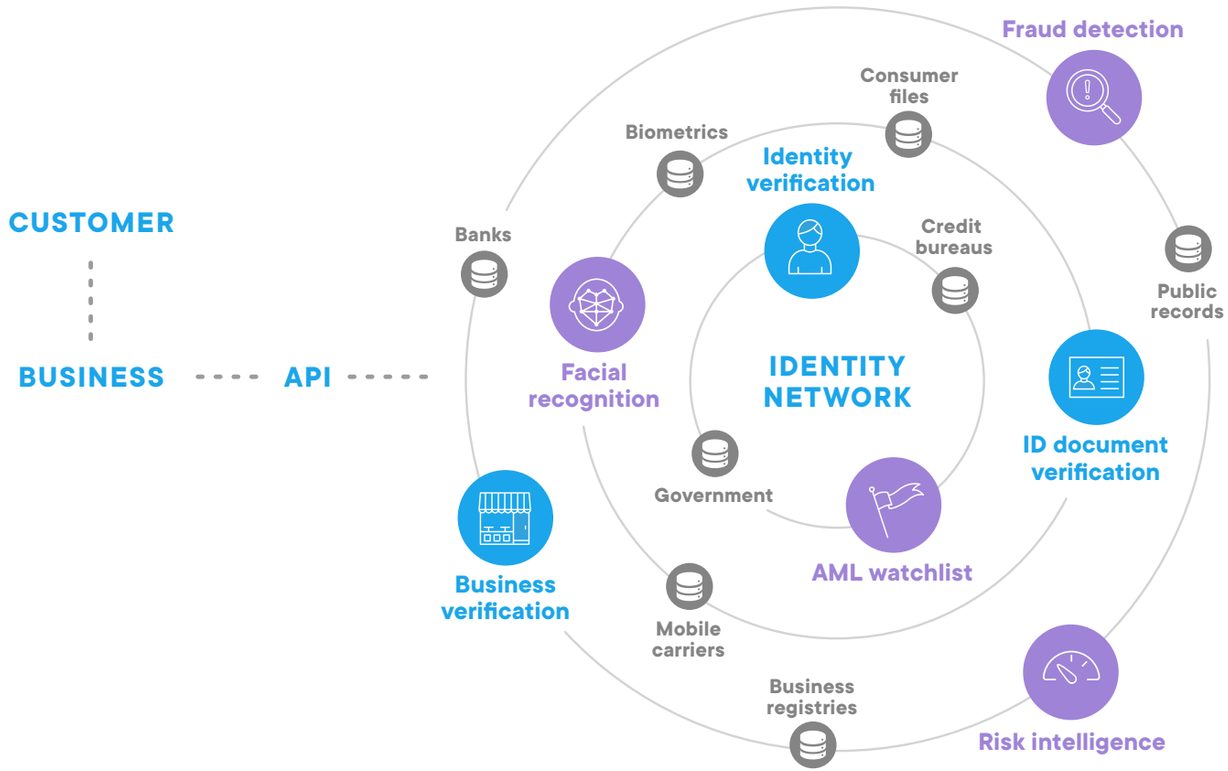
With digital access to financial services, this customer can also access the whole world of goods and services available in the digital economy.

Leveraging the API economy

The “simple” way to add a digital identity network

Application programming interfaces (APIs) are a way for companies to more easily access important business capabilities.[19]

Rather than struggling with multiple integrations or costly workarounds, businesses in the digital economy can use an API, web portal access or a low-code front-end developer tool to plug into the digital identity network. This enables them to seamlessly implement identity verification in their account creation and other processes. More importantly, the digital identity network is continually adapting and improving. Businesses don’t have to repeatedly rebuild or significantly change the customer journey to address evolving risks — the digital identity network does the hard work.



[19] Tom Taulli, *Forbes*, “API Economy: Is It The Next Big Thing?,” January 18, 2020.

Case study

A payment processor goes global in the gig economy

The unexpected rise of the gig economy has created a massive business opportunity for payment providers to provide services to new business clients. In the U.S. alone, the number of gig economy workers grew by 15% in the last decade.[20]

To manage the complexities associated with this explosive growth, a leading payment processing company operating in 40 countries needed a new, creative approach to verification. Not all gig economy workers had a business registration number that was verifiable through business verification sources. As a result, these workers were permitted to use their social security number, which would need to be verified through identity verification. The company also wanted to verify businesses through their tax identifiers, such as Employer Identification Numbers (EINs) in the U.S.

The company required a solution that would move from Know Your Business (KYB) to KYC verification under the same workflow as needed, a unique capability of digital identity networks. With the digital identity network, the payment provider is able to verify both SMBs and independent contractors in real time. In addition, the network integrates hundreds of data sources and identity verification service partners, providing a single source for the payment processor's global verification needs. The company now uses the network's expansive identity and business verification services in 36 countries and has 5.6 million transactions to date, and it continues to expand into new markets.

[20] Greg Iacurci, *CNBC*, "The gig economy has ballooned by 6 million people since 2010. Financial worries may follow," February 4, 2020.

Conclusion

Digital identity networks: Building a global ecosystem of trust for the digital economy

The internet is incomplete. Without the critical identity layer needed to build trust online, global businesses struggle with risk on all fronts: fraud, regulatory compliance, digital access and user demands for a frictionless experience. Compounding these risks is the ever-changing nature of identity.

Traditional identity solutions are likewise incomplete. For the most part, they are single-point tools targeted at one or two use cases, such as customer onboarding. They fail to answer Deloitte's "urgent"[21] call for a digital identity solution that can:

- Support transactions that are increasing in volume and complexity
- Provide seamless service delivery across all channels
- Meet regulatory requirements
- Withstand sophisticated digital attacks

Digital identity networks take the place of the internet's missing identity layer. These ecosystems of tools, services and data sources help businesses successfully navigate the changing dynamics of a global economy. As the networks adapt to address emerging fraud risks or new regulations, the business adapts too. As the networks expand their identity capabilities with new tools and data sources, the business expands too.

With digital identity networks, global companies can take a holistic view of their identity risks and use multi-layered verification to validate a user, whether that's with a government ID or a registered mobile phone in the individual's name. In this way, digital identity networks provide the assurance that businesses require to safely expand into emerging markets. These networks are also the great equalizer, enabling consumers from all walks of life to enjoy the benefits of a digital economy — which is perhaps the greatest benefit of all.

Learn more about digital identity networks and discover the right questions to ask when evaluating different identity verification solutions.

Download your Trulioo Buyer's Guide today.

[21] Deloitte Touche Tohmatsu Limited, *Picture perfect: A blueprint for digital identity*, 2016.

About Trulioo

Trulioo is a global identity and business verification company that provides secure access to reliable, independent and trusted data sources worldwide to instantly verify consumers and business entities online.

GlobalGateway, the Trulioo identity verification marketplace, helps organizations comply with Anti-Money Laundering (AML) and Customer Due Diligence (CDD) requirements by automating Know Your Customer (KYC) and Know Your Business (KYB) workflows.

Trulioo supports global clients to instantly verify 5 billion people and 330 million business entities in over 195 countries — all through a single API integration. Named as a CNBC Disruptor 50 Company, the Trulioo mission is to solve global problems associated with verifying identities by powering fraud prevention and compliance systems for customers worldwide in an effort to increase trust and safety online.

trulioo.com **1.888.773.0179** **contact@trulioo.com**