Sponsored by

Trulioo | GLOBALGATEWAY®

Facilitating trust in a shifting identity landscape

Compliance, convenience, and security through digital identity networks

In collaboration with: ONE WORLD IDENTITY

Table of contents

Executive summary

2020 has been a challenging year across all fronts for public entities, private businesses, and consumers alike.

For identity professionals and industry experts, this was the year that digital identity was brought to the forefront. The global pandemic has accelerated the adoption of digital services across industries such as eCommerce and financial services. This proliferation of digital services has intensified existing identity challenges such as the lack of strong identity verification services for accelerated digital transformation and account opening. Rapid digital transformation also caused a rise in fraud activity, with TransUnion noting an 11 percent increase from March to June 2020.[1]

Both public and private entities have recognized the growing importance of digital identity. From a regulatory standpoint, nations around the world are taking more proactive stances in governing the personal data of their citizens. These mandates (e.g., GDPR, LGPD, CCPA) largely seek to protect consumers by minimizing data collection for identity verification and improving data security. Companies seeking digital transformation must contend with a fragmented regulatory landscape of identity verification, data privacy, and data localization requirements. Digital identity networks, with access to a wide variety of trusted data sources and a comprehensive suite of identity verification services, can help businesses provide a seamless and secure user experience, minimize fraud risks, and navigate the complexities of regulatory compliance.

This paper will analyze the growing demand of digital services and how regulatory development, increased fraud activity, and changes in consumer sentiment are posing challenges for industry experts. Moreover, this paper will assess the integral role of digital identity in the modern economy, and offer an assessment on why digital identity networks are well-positioned to solve the long-standing issues that are a result of digital transformation. Lastly, we will conclude with three industry case studies — online retail, the sharing economy, and financial services — that illustrate the direct benefit of digital identity networks in solving common challenges across these sectors.

[1] TransUnion, "As More Transactions Shift Online During Pandemic, the Financial Services Industry Experiences a Surge in Fraudulent Activity," June 24, 2020

The evolution of digital identity

The perception of the digital identity industry is changing. What was viewed as a process reserved for regulatory compliance in financial services is now seen as a key enabler for improving both the user experience and fraud prevention in all industries.

Robust digital identity processes allow service providers to more efficiently discern between good users and fraudsters, provide streamlined user experiences that align with modern expectations, and meet disparate regulatory requirements. Moreover, the next frontier of digital identity solutions is focused on striking a balance between security and convenience. This section will focus on several of the key challenges — a dynamic regulatory environment, burgeoning cybersecurity issues, and evolving consumer expectations — that companies must address to develop a next-generation digital identity strategy.

Regulatory development

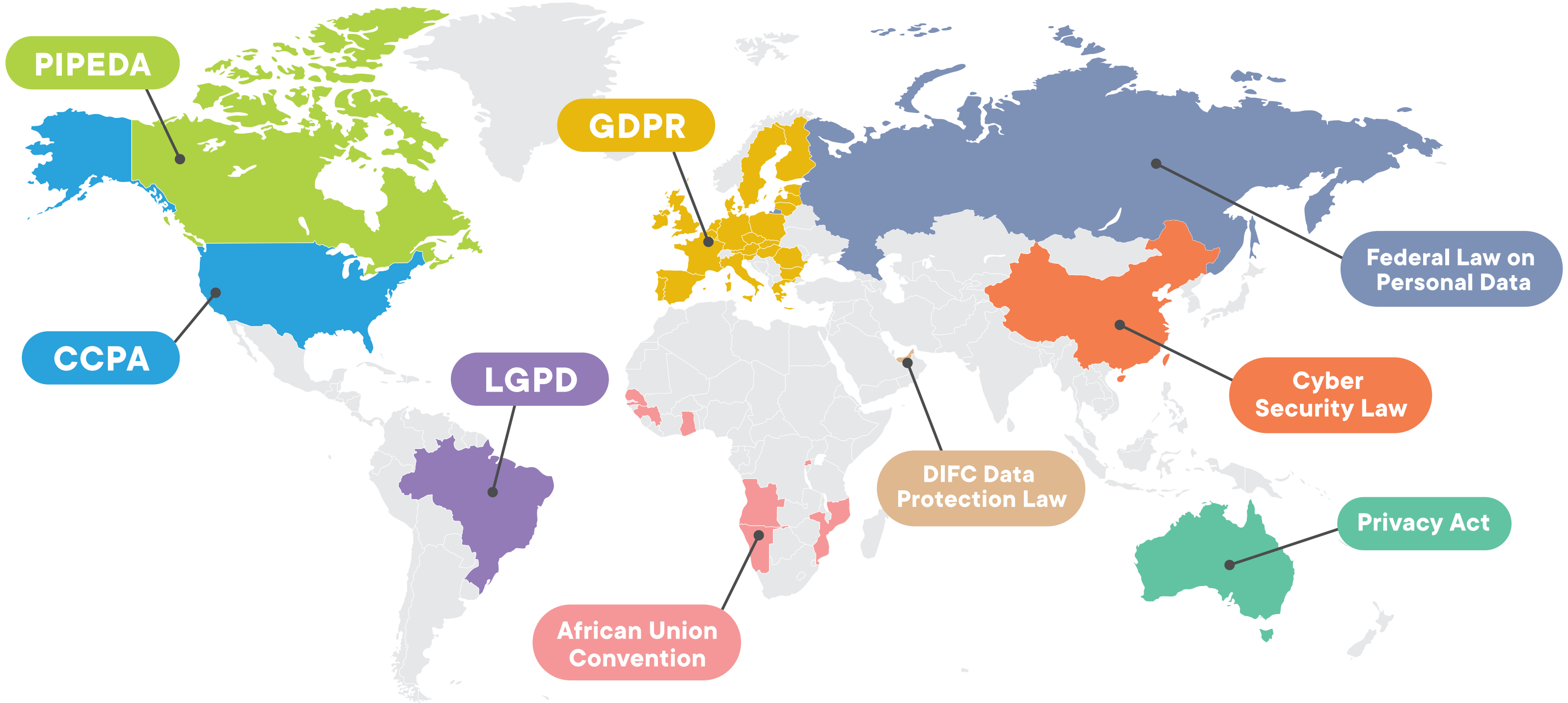
The digitization of traditionally regulated industries such as financial services resulted in a need to adopt compliance requirements for online interactions. Laws requiring identity verification are well established in western markets and are evolving with the continued adoption of digital transformation and emerging fraud vectors. The EU's 6th Anti-Money Laundering Directive will be released in December 2020.[2] Meanwhile, the Financial Crimes Enforcement Network (FinCEN) recently announced a major overhaul of U.S. anti-money laundering regulations in response to the North Korean money laundering scandal that emerged during the summer of 2020.[3] These regulations are built upon previous regulations such as the Anti-Money Laundering Directives (4AMLD, 5AMLD) and the Bank Secrecy Act, which require financial institutions to verify the identity of potential clients, understand the nature of the client's activities and transactions, and determine the potential risks of the relationship.

[2] CoinTelegraph, "Understanding the EU's 6AMLD and the risk to your business," October 18, 2020.

[3] Federal Register, "Anti-Money Laundering Program Effectiveness," September 17, 2020.

Given the sensitive nature of the information collected during identity verification, data privacy and fraud prevention strategies are crucial to lowering the risk of identity theft, data breaches, damages to brand reputation, and other fraud-related losses. Governments have responded with data protection regulations, requiring companies to give consumers insight and control over the use, storage, and sharing of their data. In 2019, California implemented the California Consumer Protection Act (CCPA), which provides Californians with new autonomy over data collected by websites. The CCPA is similar to the EU's General Data Protection Regulation (GDPR), a trailblazer for the rest of the world to follow. GDPR became enforceable in 2018 and aims to give individuals control over their personal data and to simplify the regulatory environment for international business with a unified law.

In Brazil, the General Data Protection Law (known as the "LGPD") became effective in August 2020 and provides even greater protection for consumer privacy than GDPR.[4] In addition to giving individuals the right to access and delete their personal information, organizations must provide information on who they share that data with and on how it is stored. LGPD also sets limits to international data transfers.

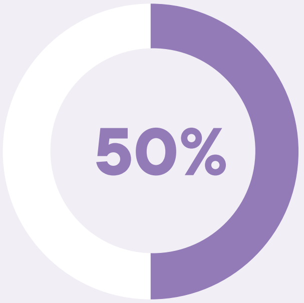


Data privacy and localization concerns are likely to remain top of mind for regulators as they work to protect consumers' data from falling into the wrong hands. According to a 2020 study by Gartner, 65 percent of the global population will be protected by modern privacy regulations by 2023.[5]

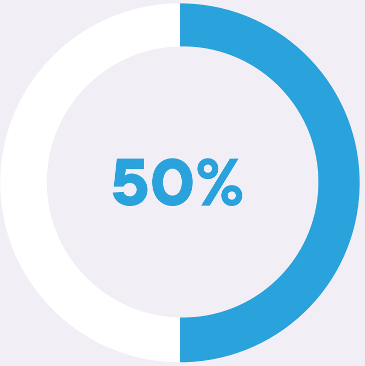
In addition to existing identity verification requirements, governments are actively exploring digital-specific regulations and frameworks. The Canadian government established the Digital Identity and Authentication Council of Canada (DIACC), a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identity framework. For easier identity verification, the U.S. Social Security Administration is launching the electronic Consent Based Social Security Number Verification (eCBSV) as part of the Improving Digital Identity Act of 2020.

[4] DLA Piper, "Data Protection Laws of the World: Brazil," January 14, 2020.

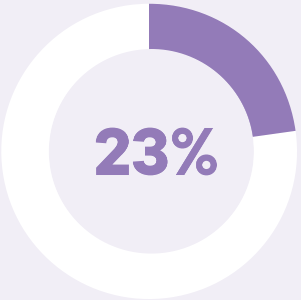
[5] Gartner, *The State of Privacy and Personal Data Protection, 2020-2022*, 2020.



Yearly increase in successful fraud attempts on retail and eCommerce platforms



Percentage of companies that have experienced a data breach



Percentage of internet users who have been victims of online identity theft

Burgeoning fraud rates and data breaches

Fraud has significantly impacted public and private entities of all sizes across every industry. Major enterprises such as Equifax, Marriott, Yahoo, and Facebook; public school systems; healthcare providers, and government agencies have all succumbed to data breaches and other threat vectors including ransomware, phishing, account takeover (ATO), and DDoS attacks. Successful fraud attempts are up nearly 50 percent year-over-year for large U.S. retail and eCommerce platforms, with the cost of fraud increasing 7.3 percent from 2019 to 2020.[6] Nearly 50 percent of companies globally have experienced a data breach at some point,[7] and approximately 23 percent of all internet users have been victims of online identity theft.[8]

In addition to growing rates of traditional fraud attacks, sophisticated new methods such as synthetic identity fraud have emerged. Sixty percent of APAC banks have experienced fraud using synthetic identities built from data stolen from social media and mobile apps, as well as from conventional sources.[9] And, as services accessible through mobile apps have proliferated, trusted phone numbers and devices are valuable targets for fraud attempts. SIM swapping, another growing fraud vector, has been around for years but has recently seen a significant uptick of nearly 250 percent in conjunction with the rise of mobile access.[10]

These threat vectors will only increase in volume and sophistication. As enterprises and individual users continue to move towards digital solutions, the demand for more comprehensive identity verification, accurate fraud detection, and stronger authentication solutions will also grow. Companies are looking not only to mitigate costs associated with successful fraud attempts, but also to prevent major reputational damage and regulatory repercussions. eCommerce, electronic payments, and financial services will continue to be attractive targets for fraudsters as end users move to mobile/digital methods of access.[11]

[6] LexisNexis, *2020 True Cost of Fraud™ Study: E-commerce/Retail Edition*, 2020.

[7] Thales, *The Changing Face of Data Security 2020: Thales Data Threat Report*, 2020.

[8] MarketsandMarkets, *Fraud Detection and Prevention Market*, 2020.

[9] LexisNexis, *Fraud and Identity Theft in Asia*.

[10] The Guardian, "Sim-swap fraud is on the rise. How can you stop it happening to you?," September 13, 2020.

[11] MarketWatch, *Fraud Detection and Prevention Market 2020-2024*, October 2020.

Changes in consumer sentiment

The uptick in data breaches, account takeover, and other fraudulent actions has raised customer awareness of data protection and privacy. Consumers are increasingly wary of corporate ownership of personally identifiable information (PII). Eighty-four percent of consumers state they want more control over the use of their data, but only 32 percent state they have already acted on protecting their data, such as paying for identity and data protection services or changing providers over careless data practices. This disparity suggests that consumers care about privacy but lack the tools and knowledge for implementation.[12]

Companies now realize that a commitment to data privacy is not merely a function of regulatory compliance, but also essential to maintaining brand reputation and retaining consumer loyalty. Trust and safety teams have emerged specifically to protect the consumer; they focus on compromised accounts, fraudulent transactions, spam, scams, and other tactics that may not be detected by firewalls and other cybersecurity methods. Trust and safety not only ensure consumer protection, but also extend brand longevity.

[12] Cisco, *Cisco Cybersecurity Series 2019: Data Privacy*, November 2019.

The future of digital identity

Digital identity infrastructure and services continue to evolve, improving accessibility to goods and services, strengthening regulatory protections, and providing new use cases for identity verification.

COVID-19 drastically sped the adoption of digital transformation, especially as companies faced the security and logistical challenges of a largely remote workforce. And consumers faced with stay-at-home orders had to rely heavily on digital solutions for daily tasks such as shopping and banking. This increased utilization of online services has driven demand for digital identity verification — 72 percent of marketplaces and 52 percent of financial services providers increased adoption of digital identity verification as a result of the pandemic.[13] To keep pace with this continued adoption, businesses are relying on new methods and data sources for identity verification, both of which are inherent benefits of digital identity networks.

Continued digitization and adoption of identity

Global demand for identity verification and fraud prevention solutions will continue to grow, especially in emerging markets like APAC and LATAM. For example, Brazil, undergoing rapid digitization, is one of the leading emerging markets for digital transformation as a result of its strong eCommerce and mobile penetration. However, the country's insecure payment systems caused a surge in card-not-present and identity fraud. A study by Konduto shows that Brazil incurred nearly $12 billion (BRL 70 billion) in online fraud losses.[14] Emerging markets will look to digital solutions to establish industry infrastructure, improve access to services, and reduce fraud, driving demand for identity verification solutions.

[13] European Business Magazine, "COVID-19 Driving an Acceleration in Adoption of Identity Verification," October 13, 2020.

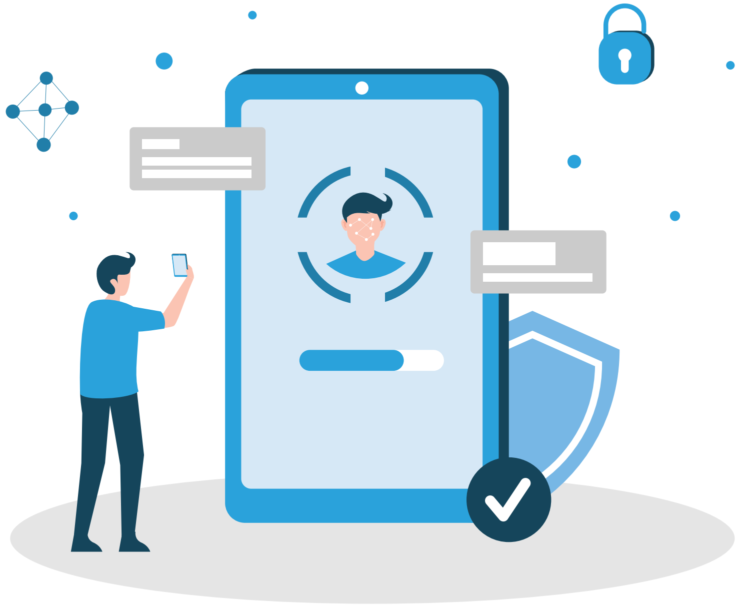
[14] PagBrasil, "Understanding Online Fraud in Brazil," March 19, 2018.

Companies are collecting increasingly sensitive and immutable data such as physical biometrics — in the event of a major data breach, consumers do not have the option of changing their fingerprints or faces. To help mitigate these risks, companies have prioritized consumer data privacy and trust and safety. In 2019, 58 percent of European companies made GDPR compliance a top priority.[15] And they're seeing positive returns on their privacy investments: Cisco's 2019 Consumer Privacy Report shows 97 percent of surveyed companies report benefits such as increased competitive advantage, better organizational agility, and greater attractiveness to investors.[16] To minimize the likelihood of PII falling into the wrong hands, companies should collect the minimum viable amount of data for their products and services, limit data transfers across borders, and leverage services such as digital identity networks to bolster their fraud detection capabilities.

The new generation of global ecommerce

The continued evolution of eCommerce has been driven by growing mobile penetration, rising marketplace fraud, and greater reliance on online retail during the COVID-19 pandemic.

eCommerce has primarily been driven by increased mobile access to goods and services, contributing to the boom of digital businesses and the digital transformation of traditional industries. Mobile channels are expected to account for 70 percent of global digital commerce by 2022,[17] and emerging economies without a mature government identity infrastructure, namely Southeast Asia and Africa, are expected to be at the forefront of mobile identity growth. Mobile-based identity is easier to scale than traditional card-based identity, as it does not require existing infrastructure, such as physical cards and registration locations. Mobile-based identity will likely be adopted as the primary identity source for more than 3 billion people by 2024.[18]



> Mobile-based identity will likely be adopted as the primary source of identity of over 3 billion people by 2024

[15] IAPP, *IAPP-EY Annual Governance Report 2019.*

[16] Cisco, *Cisco Cybersecurity Series 2019: Data Privacy*, November 2019.

[17] McKinsey, *Global Payments 2018: A Dynamic Industry Continues to Break New Ground*, October 2018.

[18] VanillaPlus, "Mobile digital identity to be a $7bn opportunity in 2024, as operators become ID brokers," September 9, 2019.

Furthermore, an increase in marketplace fraud has focused the predominantly consumer-centric industry on seller verification.[19] Given the influx of small and medium-sized businesses moving online and the popularity of online marketplaces like Amazon and eBay, demand for business verification is growing to ensure the legitimacy of sellers in two-sided marketplaces.[20]

Finally, stay-at-home orders due to COVID-19 kept consumers out of physical retail stores, causing digital retail to skyrocket. As of April 2020, year-over-year global online retail sales were up 209 percent.[21] In the absence of in-person shopping, consumer demand for convenient checkout services, such as one-click ordering, mobile access, and curbside pickups, all hinge on a seamless yet secure user experience. According to IBM's U.S. Retail Index, the COVID-19 pandemic has accelerated the shift to eCommerce by five years and is projected to grow nearly 20 percent in 2020 alone.[22]

[19] Simility, "Online Marketplaces: The Hotbed For Fraud," August 28, 2018.

[20] eGrowth Partners, "Amazon Sellers Failing Account Verification at Record Rates," May 22, 2020.

[21] ACI Worldwide, "Global eCommerce Retail Sales Up 209 Percent in April," May 12, 2020.

[22] IBM, *Meet the 2020 Consumers Driving Change*, 2020.

Alternative data and innovative methods of identity verification

The evolution of digital identity has required organizations to find innovative ways of verifying identities and detecting online fraud. For example, more and more identity service providers are leveraging a mix of both traditional and non-traditional data sources. Traditional data such as credit scores, financial history, and utility/housing history restricts reach to specific demographics and may not work for "thin-file" users — those with insignificant or no credit history.[23] On the other hand, alternative data sources such as user and entity behavior analysis (UEBA) and mobile/device intelligence help enable fraud detection without adding friction.

UEBA is a relatively new market that developed in response to the increased collection of consumers' online activity and the mainstream application of machine learning. UEBA solutions look at behavior patterns of human users and entities (such as routers, servers, and endpoints) to detect meaningful anomalies that indicate potential threats. UEBA expands upon traditional cybersecurity tools by detecting suspicious behavior based on pattern recognition. Strong UEBA solutions are able to detect complex attacks across multiple users, devices, and IP addresses.

> **To verify identities and detect online fraud, more and more identity service providers are leveraging a mix of both traditional and non-traditional data sources.**

Like UEBA, mobile identity and device intelligence enable a seamless layer of fraud detection by using mobile devices as unique identifiers to authenticate users and track ongoing platform activity. Mobile identity is made up of phone numbers, plus associated names and addresses, and device information includes location data, device ID number, and SIM card ID. Mobile identity providers are also able to analyze risk signals based on data they collect from these two sources to track anomalies and detect future fraud.

Furthermore, fraud detection methods have grown to encompass intra- and inter-company connections. These methods leverage internal product suites and external partnership networks to proactively inform companies of suspicious behavior of a user's digital credentials across a variety of platforms. Well-connected identity solution providers such as digital identity networks can use a variety of identity products and services to provide a comprehensive identity overview for verification and monitoring, flagging suspicious activity and alerting other participants within the network.

Finally, public and private entities alike are exploring the potential for decentralized identity, which shifts identity ownership from a central party (government or private organization) to consumers themselves. This provides users with greater control over their data, establishes interoperability among organizations, and removes the centralized "honeypot" of PII so attractive to fraudsters. One example of decentralized identity is self-sovereign identity (SSI), which fully distributes all digital identity attributes, ownership, and responsibilities to the user. The individual retains complete control of their digital identity credentials and identity data. SSI differs from current methods and practices by the use of a secure distributed ledger technology and through its adherence to a set of ten guiding principles set by Christopher Allen, a pioneer in decentralized identity.[24] The success of decentralized identity is yet to be determined — major hurdles like regulatory acceptance, user education and adoption, and vendor buy-in stand in the way of widespread use.

[23] One World Identity, *Bad Credit? No Credit? Big Identity Problem: The Definitive Primer on Identity Data in Credit Scoring*, July 2017.

[24] Life with Alacrity, "The Path to Self-Sovereign Identity," April 25, 2016.

Digital identity networks and the future of eCommerce

Mobile penetration and COVID-19 have significantly accelerated the expansion of eCommerce. This growth has been met with a commensurate increase of fraud.

Account takeover fraud rates grew by 282 percent from Q2 2019 to Q2 2020, with overall fraud attempt rates rising 1.6 percent year-over-year to 5.3 percent in Q2 2020.[25] As companies struggle to find the balance between minimizing consumer friction without sacrificing security, digital identity networks have emerged to provide a holistic, streamlined approach to managing risk.

The development of digital identity networks

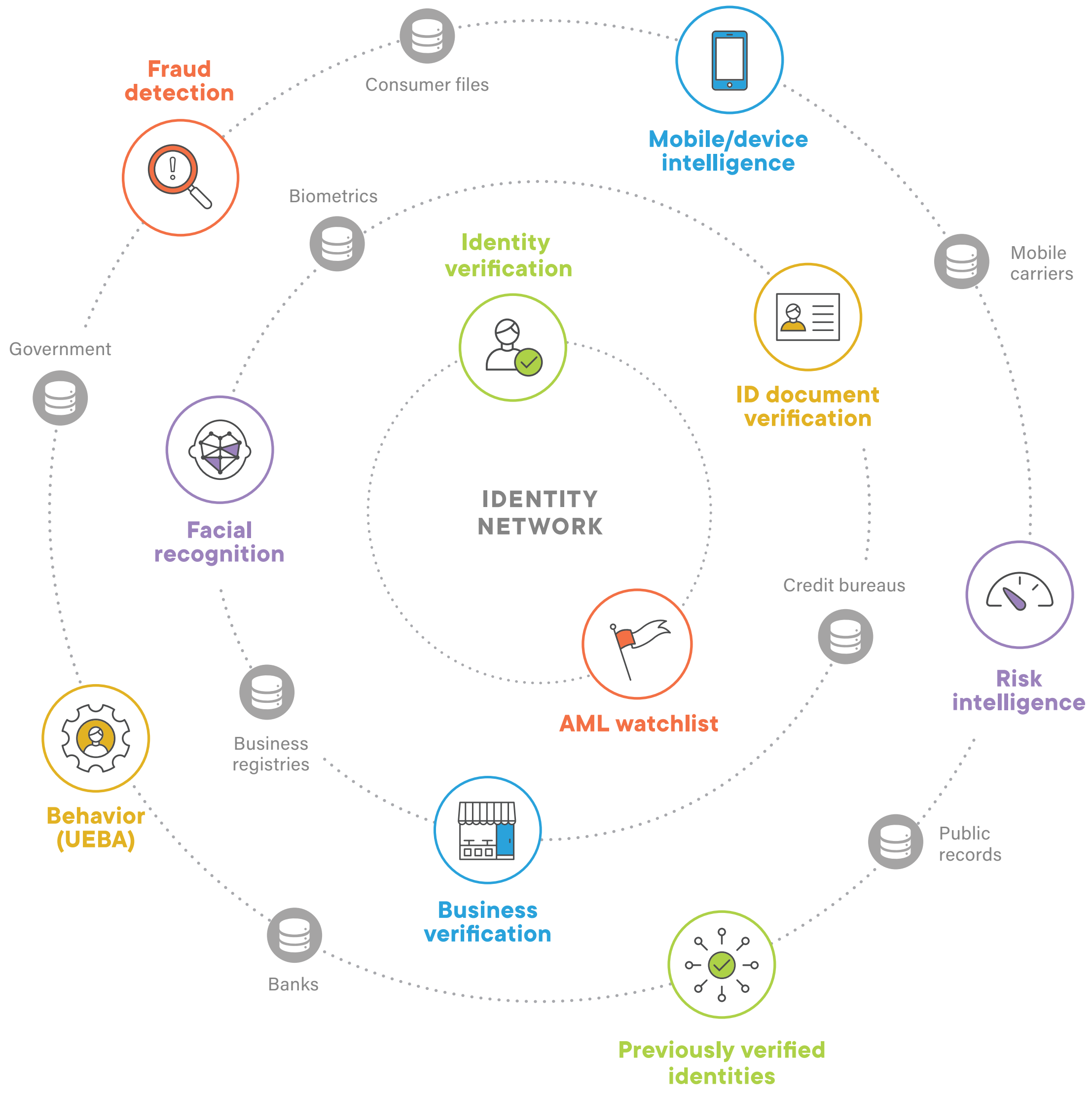
Traditional identity verification services are typically point solutions that rely on verification of identity attributes against documents issued by trusted sources. They often require manual review and do not incorporate alternative data, device intelligence, or other qualitative risk indicators.

Digital identity networks emerged as an improvement on traditional, static identity verification methods. They help businesses manage risk while accounting for the constantly evolving nature of digital identity by providing a holistic view of traditional and alternative data attributes from a variety of trusted sources.

Digital identity networks access a variety of trusted sources and data types — such as government agencies, telecommunications providers, credit bureaus, watchlists, mobile numbers, email addresses, and previously verified identity credentials — for identity verification. Leading digital identity networks are differentiated by:

- The various types of verification services they offer
- The depth and breadth of data sources they can access
- The ease with which customers interact with the service
- The security and reliability of the platform

[25] ACI Worldwide, "Global eCommerce Retail Sales Up 209 Percent in April," May 12, 2020.



Effective digital identity networks lower user friction by enabling businesses to collect the minimum number of data attributes needed to meet the desired level of identity assurance, leveraging previously verified credentials and incorporating non-traditional identity attributes such as mobile and device intelligence in calculating the risk of an applicant.

The evolution and proliferation of digital identity has improved accessibility and convenience. However, there has been a corresponding increase in the volume of valuable identity data for fraudsters to exploit. Successful digital identity networks improve efficiency and reduce risk for businesses by providing a comprehensive, secure suite of identity verification services with access to a variety of trusted data sources. They also enable companies to collect the minimum amount of information necessary to verify identities, reducing the volume of sensitive identity data and addressing data minimization regulations emerging around the world.

> By proactively preventing fraudulent activities, digital identity networks are key to establishing and maintaining trusted relationships between businesses and consumers.

Use cases: opportunities for enhancement

A digital identity network can quickly and intelligently adjust to suit any business context, enabling companies to verify identities of individuals and entities through data verification, physical and behavioral biometric matching, and customizable rules engines. These features culminate in an agile, optimized solution that leverages a diversity of data types and sources to conduct identity and document verification, identify and verify ultimate beneficial ownership, and mitigate fraud in a compliant, secure manner.

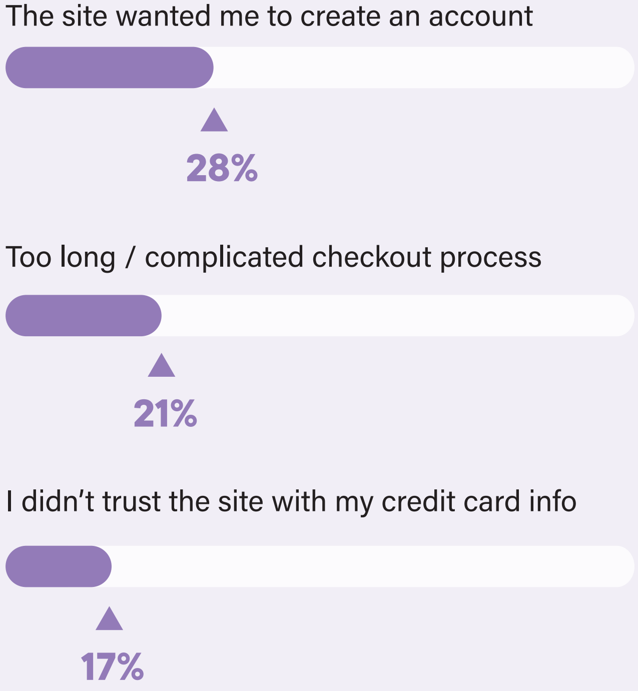
Trust and safety for consumers can be established through risk-based workflows that streamline verification and authentication processes for low-risk identities while maintaining additional layers for higher-risk cases, improving user experience. Furthermore, network intelligence and communication enable greater insights across disparate services and sources, allowing for improved data portability and credential interoperability. Digital identity networks are beneficial across a wide spectrum of use cases and industries to improve security, reduce friction, and maintain compliance.

Online retail: security without friction

The global burgeoning of online retail is not without its challenges — 69 percent of digital shopping carts are abandoned, with 28 percent of abandonments due to mandatory account creation for checkout (as opposed to checking out as a guest), 21 percent as a result of a complicated checkout process, and 17 percent due to lack of trust in website security.[26] Online retail providers must balance collecting sufficient data to minimize fraud risk with a streamlined checkout process.

Digital identity networks can operate without consumer input to assess behavioral biometric data and device metadata in real time, minimizing the user burden of proof. Companies can provide a convenient checkout experience while still verifying the authenticity of the transaction, minimizing friction to enable a smooth user flow.

Reasons for abandonment during checkout process



[26] Baymard, "41 Cart Abandonment Rate Statistics," September 10, 2019.

The sharing economy is set to reach a market size of $335 billion by 2025

Sharing economy: seamlessness and customization

The sharing economy has witnessed explosive growth and is set to reach a market size of $335 billion by 2025.[27] With this growth comes intense competition and identity verification challenges in an industry filled with complexities and nuances. Sharing economy providers must not only maintain vast quantities of user profiles and identity data but are also legally required by some jurisdictions to conduct background checks on gig workers and authenticate workers during shifts. Sharing economy companies must contend with as much as 500 percent churn of workers year over year, incurring significant costs for identity verification.[28] Furthermore, verification of individuals differs from verification of businesses — the process may be conducted based on a wide variety of data points, especially for companies operating across jurisdictions.

Based on the variable identity data attributes provided, digital identity networks provide custom workflows for real-time identity verification for both merchants and gig workers. The ability to implement interoperable workflows to authenticate and verify variable data points for multiple use cases enables a seamless onboarding flow for users. By facilitating the verification of all users in a digital ecosystem, digital identity networks help establish the trust and transparency that sharing economy companies need to attract and retain users.

Financial services: meeting compliance requirements

Financial services providers must comply with complex KYC requirements to prevent money laundering, terrorism financing, and other financial crimes and fraud. The emergence of fintech and other digital disruptors has accelerated the push toward the digitalization of KYC and KYB processes, especially for a growing class of Money Service Businesses (MSB) that are also subject to KYC regulations.

A digital identity network can provide a single point of access for KYC and KYB, simplifying the process of AML/CFT compliance requirements. The digital identity network can also simplify the complexities of a tech stack consisting of third-party vendors that cybersecurity, compliance, and trust and safety teams use and maintain. Through digital identity networks, financial services providers and fintechs can also drive diversity, accessibility, and inclusion by reaching a wider audience that may have previously been excluded through traditional identity verification.

[27] The Balance SMB, "The Sharing Economy and How it Is Changing Industries," June 25, 2019.

[28] Wall Street Journal, "In a Tight Labor Market, Gig Workers Get Harder to Please," May 4, 2019.

Conclusion

Rising fraud, concerns around data privacy, and an increasingly complex regulatory landscape have brought urgency to the adoption of digital identity and identity verification.

As public and private entities continue to undergo digital transformation, regulations, standards, and guidelines will continue to change to address new use cases. Likewise, fraud attempts will become more sophisticated to overcome existing detection and prevention methods, and, left unchecked, will erode consumer trust in digital services.

Digital identity networks can help businesses navigate this constantly changing digital identity landscape, providing a holistic view of user identities and risk factors and bringing greater accessibility to digital services. They can also smooth the challenges posed by unprecedented global crises and ensure that focus is on improvement, rather than repair. Businesses seeking to undergo digital transformation should leverage digital identity networks to engender consumer trust, mitigate business risk, and enable continued growth, convenience, and inclusion.

Trulioo | GLOBALGATEWAY

The digital identity network

A holistic approach to managing risk in a global economy

trulioo.com

Thrive in the digital-only economy.

Intelligent use of identity networks yields competitive advantages for businesses at all stages of growth.

Download the Digital Identity Network Reference Paper

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**

About One World Identity • OWI is a research and advisory firm focused on identity, trust, and the data economy. We help businesses build solutions, execute upon strategies, invest intelligently, and connect with key decision makers. Every day, billions of interactions track the identity of people, entities, and things. We think of digital identity not as a what, but a how; it's the hidden fabric enabling the seamless exchange of trusted information at the scale and speed required by global enterprises. We believe digital identity is the linchpin to digital transformation. Done well, it can provide inclusion, privacy, and safety. That's why we've dedicated ourselves to solving its challenges.

🖥 **oneworldidentity.com** ✉ **info@oneworldidentity.com**

Disclaimer: Trulioo provides no warranty that the information contained in this document is accurate, up to date or complete and in no circumstance does such information constitute legal advice. Any person who intends to rely upon or use the information contained herein in any way is solely responsible for independently verifying the information and obtaining independent expert advice if required.

Copyright © 2020 Trulioo Information Services Inc. All rights reserved. This document is classified Public. Trulioo, GlobalGateway, Building Trust Online, and A Snippet of Code, Verify the Globe are either registered trademarks or trademarks of Trulioo Information Services Inc. in the United States and/or other countries.