KNOW IDENTITY

The Evolution of Identity Verification in the Marketplace

WHITEPAPER

January 2021
Digital Roundtable

Presented by:

ONE WORLD IDENTITY

Trulioo

TABLE OF CONTENTS

03 Abstract

04 Key Takeaways

05 Rising Regulations: Navigating a Sea of Shifting Compliance

09 Building the Trust: Changing Marketplace Dynamics

13 Personal Privacy: Evolving Consumer Sentiment

16 Conclusion

17 About

18 Contributors

Roundtable Moderators

Cameron D'Ambrosi - Managing Director at One World Identity
Zac Cohen - COO at Trulioo
Stephen Ufford - Chairman of the Board at Trulioo
Rutherford Wilson - VP of Emerging Technology at Trulioo
Asya Bradley - Founder & COO at First Boulevard
Don Cardinal - Managing Director at Financial Data Exchange
Shivendra Kishor - Head of Fraud, Identity & Abuse - Analytics & Operation at Lyft
Jas Randhawa - US Compliance Officer at Stripe
Grace Wu - Head of Risk Partnership at Uber

ABSTRACT

In the month after the September 11, 2001 attacks on the World Trade Centers and the Pentagon, the US government passed the USA PATRIOT Act, a wide-ranging, well-documented law that put in measures to prevent future terrorist threats. Almost overnight, Know Your Customer (KYC) became a highly important measure, particularly in banking. The PATRIOT Act required financial institutions to create a Customer Identification Program and conduct customer due diligence for KYC.

This law ushered in the modern effort to verify and confirm customer identities, whether online or in person.

While the act was built to combat terrorism, it shaped the way banks, retailers, and the general marketplace fights fraud. As this KYC grew to encompass the rise of the online marketplace, its application has also expanded to target digital identification, fraud protection, and understanding the characteristics of their customers without overstepping privacy concerns.

OWI's most recent roundtable addressed this evolution in the marketplace through lively discussion about how fraud prevention efforts have evolved, where major consumer concerns lie, and the methods by which companies have taken the mantle to build out these digital identities. These conversations revealed that while organizations have made major strides in identifying users, there remains many gaps in these efforts. Challenges to identity verification in the marketplace are driven by the scarcity of industry- and region-agnostic regulation for identity interoperability, limited understanding from consumers about sharing data and how it relates to privacy, and the overarching impact of the COVID-19 pandemic on digital transformation and adoption.

From these discussions, three important themes emerged:

- Compliance officers need to focus on "tools and rules," or technology to allow for flexible and innovative tailored solutions to navigate regulations while also remaining up to date on the latest laws, where change is unavoidable

- The rising tide of online transactions has shown a corresponding increase in fraudulent activity. Companies need to find solutions to mitigate fraud and identify bad actors as the online shift has created a new baseline for business and will not disappear any time soon

- Customers want some level of "positive friction" when verifying information, such as responding to a biometric identifier (like a fingerprint) or incorporating a code sent via a text. Transparent terms and concise data requests provide a few ways to reduce the risk of customer drop-off

KEY TAKEAWAYS

1. Regulators across the world have not come to a consensus about how to protect privacy and enable cross-border digital identities. This patchwork of regulation and compliance requirements generates friction and confusion as companies expand into new regions.

2. Adjust KYC measures to the changing regulatory landscape by finding technology that can grow as the organization grows, having a proactive compliance officer, and ensuring flexibility in the company's infrastructure design.

3. The increase in online-only systems, particularly among industries slow to undergo digital transformation, has led to a significant increase in fraud during the pandemic. This can further deplete customer willingness to provide data to an organization.

4. The seesaw battle between frictionless sign-ups versus ensuring a secure experience does not need to occur. Instead, return to the digital identity and KYC tools and seek solutions that blend the two concerns into one strong experience.

5. The consumer privacy paradox highlights how little a regular user understands or has interacted with digital identity tools. The opportunities consumers have to interact with digital identity tools have increased, creating an opening for organizations to better educate and guide customers.

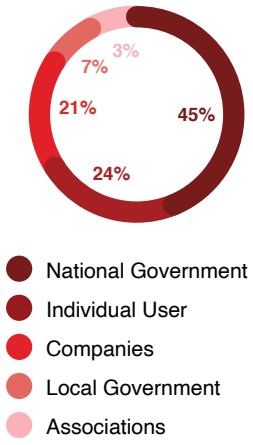
RISING REGULATIONS: NAVIGATING A SEA OF SHIFTING COMPLIANCE

The roundtable discussion began with a conversation about how to navigate the various regulatory frameworks, which companies have to comply with as they cross borders and grow internationally. While organizations want more transparency and interoperability to improve processes, any true comprehensive plan from government regulators could be years in the making. Instead of comprehensive standards to digitize and verify identities, whether through centralized, independent service, a decentralized ecosystem, or from legislation that provides guidance on what organizations can track, measure, and keep within their own systems, what has developed is a piecemeal response to digital identity that differs based on the region or country of operation.

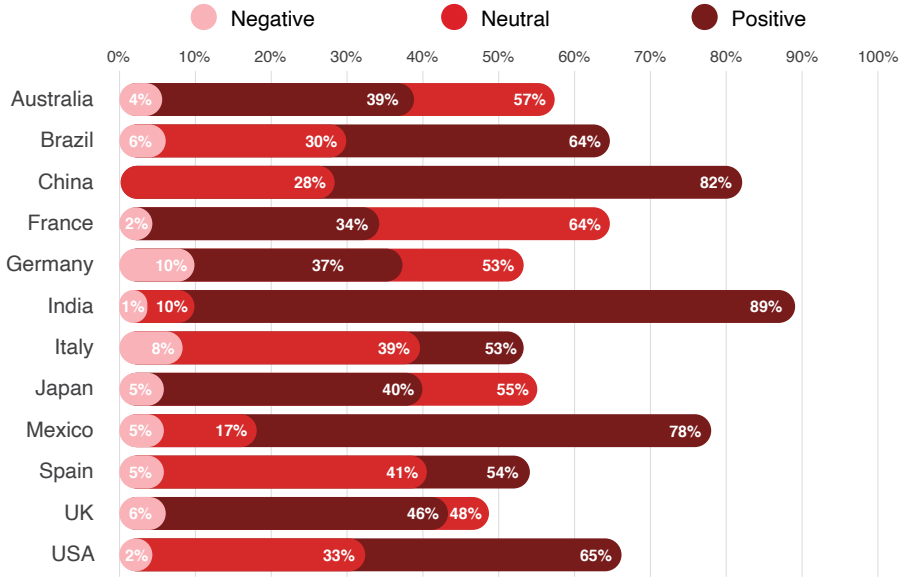
Take for instance the General Data Protection Regulation (GDPR) passed in 2018 in the European Union (EU) to provide some privacy parameters. It enforces some rules that a consumer appreciates when it comes to privacy protections. It requires a need for a purpose to hold the data, it must be limited to the data needed for the specific purpose of use (and nothing more), and it sets limits on how long the data can be held. This has become the modus operandi in Europe. However, US firms must comply with a different set of regulations for domestic operations. Companies serving customers in California or those storing a significant amount of Californians' data must comply with the California Consumer Privacy Act (CCPA), which provides some of the regulation and protections that GDPR does, but differs in many ways as well, including:

- The GDPR has more restrictions on data processing
- The GDPR does not assume that consumers give permission, while the CCPA requires consumers to opt-out, assuming permission of data gathering
- The CCPA requires that companies provide information about where the data was sold within the one calendar year[1]

Who is Primarily Responsible for Protecting Data

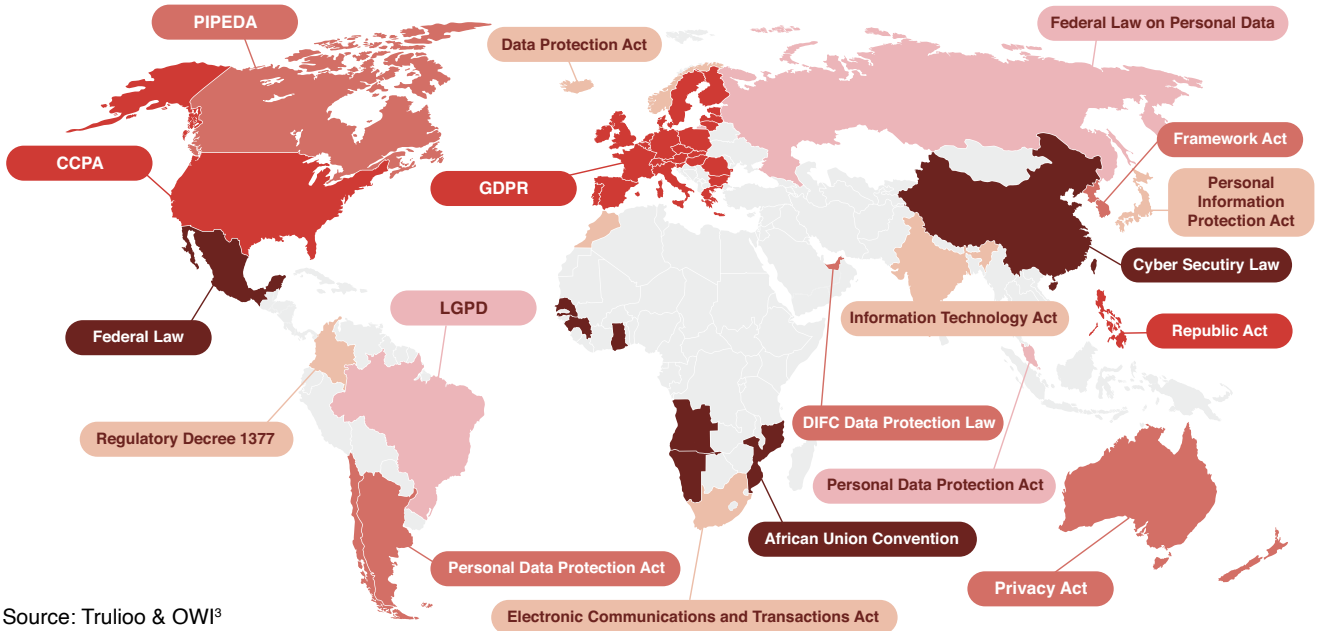


Overall Sentiment Regarding the Impact of GDPR



Source: Cisco Consumer Privacy Study[2]

Both GDPR and CCPA give consumers some rights to opt out or delete their personal information. Of course, these are not the only two forms of regulation that touch on digital identity and KYC, even within these two specific regions. In the fraud and money laundering space, for example, the 5th Anti-Money Laundering Directive (5AMLD) governs the EU. In the US, the Senate has proposed the INFORM Consumer Act, which would force retailers to verify the identities of their largest sellers, bringing in questions about how to best do so, and why. Meanwhile, each individual state can pass their own version of a CCPA at any time. Then there is a global movement to increase regulation over all of Big Tech, driven by momentum from the nonpartisan supporters, such as some Democratic lawmakers, former President Donald Trump, and German Chancellor Angela Merkel. Depending on the legislation that takes shape, companies may need to adjust their identity efforts even further, continually evolving with new laws in order to remain in compliance with emerging requirements around identity verification and data collection.



Source: Trulioo & OWI[3]

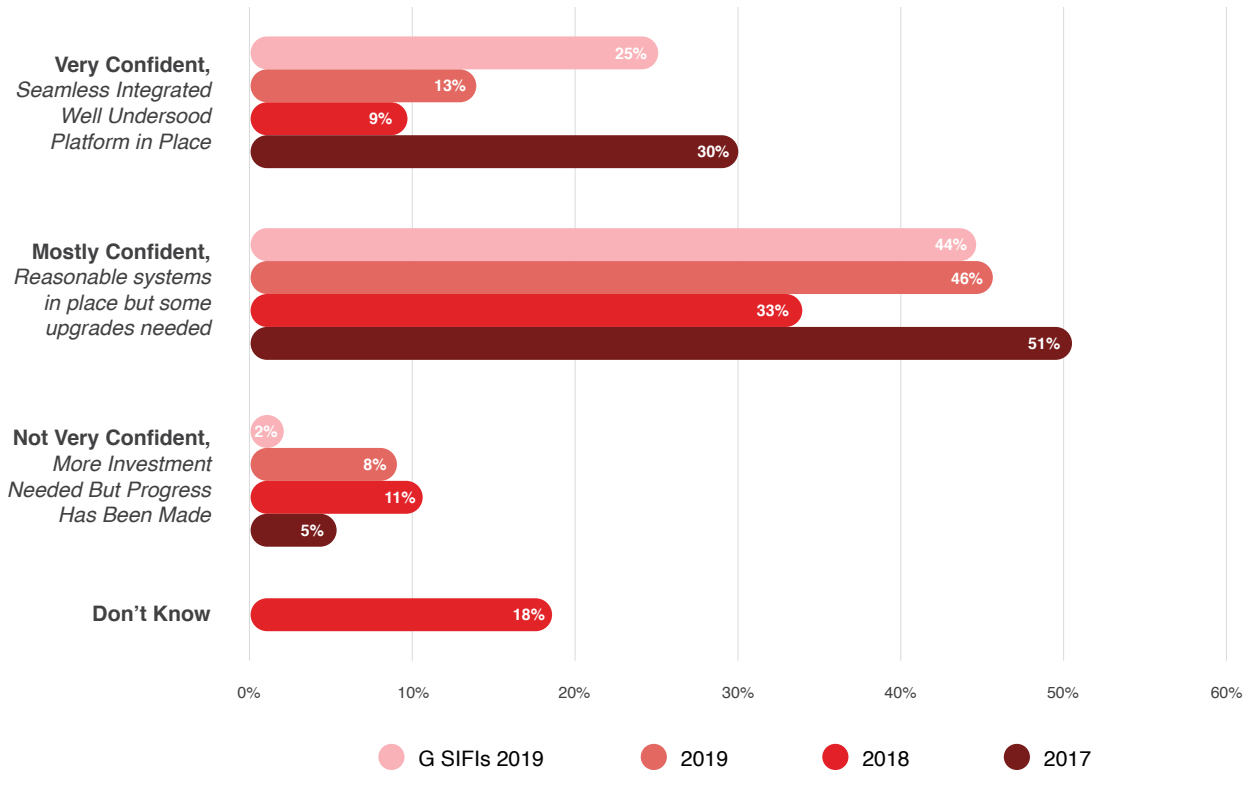
KYC's Regulatory Impact

When regulators first began to oversee the Internet, they sought to regulate a global tool with traditional tactics built with national or local concerns in mind. However, regulations that worked on offline entities don't translate well for digital providers, where many companies operate with an international range of customers. Compliance becomes particularly difficult with regards to KYC and data privacy, since rules differ so widely based on the country or region. The inability to understand, track, and ensure compliance across borders can lead a startup or growing company to plateau or fail.

KYC plays an important role in preventing fraud and money laundering for certain sectors, but it runs up against significant limitations due to privacy regulations. Organizations must ensure they only collect relevant data or information necessary to understand who their customers are for fraud prevention, money laundering, and identity theft protection, without overstepping the laws of the jurisdiction, region, and country.

Solving this issue requires the proper technology to create digital identities for users, as long as there remains no central resource for the digital identities, which remains the case for the foreseeable future.

How Confident Are You That Your IT Infrastructure is or will be Able to Support Fintech, Regtech and Insurtech Solutions?



Source: JD Supra[4]

How to Adapt

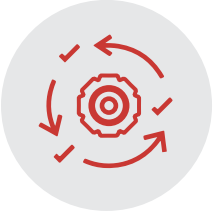
No matter the sector, a startup or growing business cannot circumvent KYC and data privacy regulations. By showing an ability to lead in an industry, however, the success can encourage regulators to seek a company's advice as governments build out plans for oversight. There are clear advantages to having this position with regulators. Whether or not that occurs, taking steps to better protect against future regulatory changes, such as increasing control consumers have over their data, and protecting growth from compliance differences as the business moves across borders, has value today. To do so requires foresight and investment in these key areas:

Address Technology For Future Use

By utilizing the right technology and digital identity tools, the company can ensure a system that can grow with the organization. It requires future proofing your solutions by accessing technology and partners that provide scalability, interoperability, and flexibility as a company expands into new countries and regions.

Hire a Proactive Compliance Officer

In the past, compliance officers often served as an almost judge and jury of what a company can do, providing a yes or no verdict depending on the technology and laws. Now, they require a proactive mentality for implementing technology that supports the company's current and future goals; communicating with customers, clients, vendors, and regulators; and establishing a compliance framework that supports and protects company decisions. This proactive approach ensures the company can adapt to changing compliance requirements, especially if regulators audit the firm.



Maintain Flexibility

Though companies cannot control the evolution of the regulatory landscape, they can build with tools that will scale with company growth and update to comply with new requirements. By maintaining this "tools and rules" mindset, a company's compliance structure will not face foundational challenges even as rules change, since the vendors will track such shifts in the market, catching issues that the organization does not.

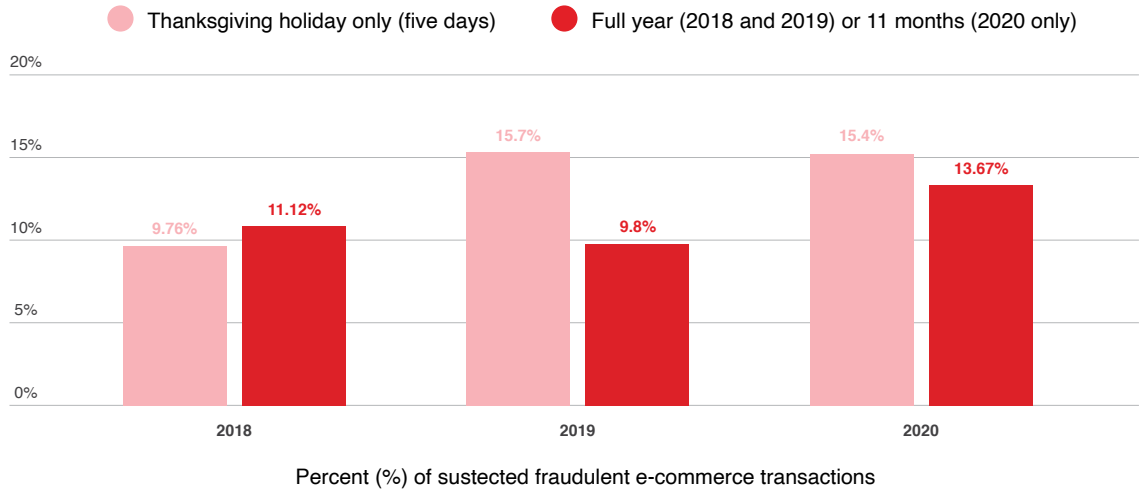
As regulations shift, organizations will have to move with the laws. But the proactive approach to compliance, through technology and having the proper vendors, will allow the business time to adjust, since fewer surprises will exist.

BUILDING THE TRUST: CHANGING MARKETPLACE DYNAMICS

In March 2020, the world was thrust into a unique experiment. Due to the COVID restrictions, including stay-at-home orders, organizations had to adjust to the new normal of interacting with customers from home, building in work-from-home capabilities, addressing all sorts of healthcare issues, and improving educational systems. Many consumers shifted to online-only when it came to banking, purchasing, or healthcare for the first time. For digital first companies, they were already prepared for such a world. But plenty of other firms were not. This confusion and mass adoption of the online tools led to a significant increase in fraud.

In the US, these fraud efforts varied. Banks have reported scams on stimulus payments Congress passed in March and December. The Federal Trade Commission has said that more than 327,000 complaints flowed into its office in 10 months.[5] Phishing scams also saw a significant uptick. This trend bled into the holidays as well, which saw a 14% increase in e-commerce fraud through the early part of the holidays when compared to 2019 and a 59% increase from 2018, according to Transunion data.[6] More must be done at the organizational level to protect customers and the company from these efforts.

Holiday E-Commerce Fraud is on Par with Last Year, But Up Overall



Source: Transunion[7]

While fraud has risen under the COVID digital adjustment, the trust that consumers have in sharing their information in order to prevent such practices has fallen. Even as 76% of consumers believe that sharing personal information is a necessary evil in today's world, 85% wish there were more companies that they could trust with their data.[8] This becomes a tough balance because companies need to ensure customers' digital identities, but customers do not trust companies to do so or do so in a way that will keep their information safe.

Organizations face this uncertainty from consumers while also trying to develop frictionless systems to ensure customers do not leave signup processes early. Among consumers of financial services or online gaming tools, 77% report that the account opening process can "make or break" their future relationship with a brand. If there are too many steps required to confirm someone's identity to load them into the system, then the user will not engage with the tool to the levels these organizations need.[9] The most sophisticated technology does not require a balancing act between friction in the system and security, but rather implements a balanced digital identity process to ensure user verification while also protecting the security by only holding onto the data required to confirm the identity.

The security of the data is one layer to ensure a clear picture of customer identity, while preventing fraud. Some of the other potential shortcomings, include:

Limited Consumer Understanding – While consumers want speedy service, they often need an understanding of why the data is needed to improve the experience. At the same time, they do not want to have to read a legal document or go through the process of selecting what data points are needed simply to check a website or sign onto an app. An effective solution should educate consumers in an easily understood and digestible manner to establish a relationship based on trust and transparency.

User Data Control and Interoperability – Consumers have little control over their data, how they can use it, and when they can take it away. The ability to shift or erase data across platforms, regions, or countries would improve this capability and produce a more accurate digital presence that reflects the person today. Organizations can improve this as well by only utilizing data that is necessary to produce an accurate digital identity instead of seeking unnecessary information. Advanced diagnostics and AI tools that provide more accurate measures of identity can help limit the amount of secondary and tertiary data held.

Data Silos – Too often, as companies or even segments of organizations have built in efforts to track digital identities, they have tried to go it alone, as opposed to utilizing a central internal resource, leaning on an external group, or participating in an industry-wide effort. The more data available to cross reference and support, the stronger the identities that develop when using advanced diagnostics, AI, and machine learning. The more partnership incorporated into the program, the greater the ability to ensure strong digital identities across the organization, industry, or markets.

Sophisticated Fraud Schemes – Criminals always look for new ways to circumvent protective measures. One new tactic involves developing a synthetic identity using a mishmash of real data with fake features. Use of these Frankenstein-like identities can allow a criminal to pose as a real person for years, and account for about one-fifth of credit losses to fraud.

Old Fraud Tactics Remain Viable – Even as the growth of unique fraud efforts rise, many organizations also have not taken steps to stop the easiest of illegal tactics, such as phishing or imposter scams, which remain among the most common types of fraud reported to authorities. Such irresponsibility leaves the company at risk and further depletes consumer confidence.

Like any business, those committing fraud run a cost-benefit analysis to determine if efforts to breach a system are worthwhile from a financial standpoint, based on the cost and risk involved. Improving and expanding on a unified and transparent digital identity ecosystem creates a much higher hurdle for fraud, not only reducing the likelihood that the effort will succeed but making it far more expensive to even try.

To accomplish this feat requires a robust digital identity effort, including strong KYC and an array of identity verification and fraud prevention technologies to properly identify people – whether they are fraudsters or not – without leaving data at risk of security breaches or lacking privacy controls. Such systems, whether developed in-house or via a larger organizational presence, achieves many of the company goals of fighting fraud, while also easing consumer concerns. Such a design can also provide insights into your organization, finding opportunities that in the past would have disappeared. A loan originator, for instance, could identify the root cause of a declined application. With more insight, it may turn out the application should have moved forward, declined because of a minor issue in the person's background. Such a system allows for a stronger customer base, which can work for credit card companies, banks, peer-to-peer lenders, and many other financial firms and offerings.

Even in such a design, it requires direct and transparent communication with customers so they understand why they should share their data.

Part of fighting fraud involves utilizing various new forms of data that could not be tracked or acted upon in the past. This provides an opportunity for this alternative data to better offer fraud actions, prevent new strategies, and scare away old tactics for good.

Mobile Identity and Device Data – How people use their devices and share information on mobile tools creates a unique signature and serves as an extension to digital identities. Utilizing this signature and data can aid in ensuring the person logging into the account owns it, but also better identify the same person as they move to other retailers, networks, and financial institutions.

Behavioral Biometrics – Users develop specific and identifiable patterns as they move online. Now, with the ability of big data and AI, technologies can identify that behavior and link it to the correct digital identity. If the behavior sways in any way, then a potential fraud has been detected based on the past behavior, since it becomes almost impossible to mimic by a third party.

Transactional Data – Tracking someone, whether a person or institution, by name to confirm a purchase or identity has downsides. Fraudsters can more easily fake the name. But utilizing transactional data to identify an organization or person, without having to know anything else about the person, can provide a clear digital identity, one that surpasses the name. The same can work with bank data, since customers trust the security of that data and institution more than nearly any other entity.

The inability to correctly identify someone in the financial sector because they have a thin profile when it comes to their credit analysis has long been a shortcoming of the credit industry. Immigrants new to the US struggle to open a credit card, even if they have a long history of paying their bills in their homeland. Or someone who has lived in the US for a number of years and done well from a financial standpoint, if this person came from a less advantaged country then they can face significant hurdles to sign up for the simplest of purchases. The same can be said for those with a weaker economic prospect, since the tools to measure credit scores track standard banking tools and debt levels. Someone in a poor economic situation may have only a thin amount of data to support the credit check, leading to a rejection even in situations where they would make for a quality customer.

The Policy & Economic Research Council found that a reduction in the use of alternative data during credit checks led to a 37% lower approval rate for people in lower-income households without any change to the overall risk profile of the institution.[10]

Such designs create disparities in the financial space. In essence, it does not pay to ignore these buyers, nor does it materially increase risk levels. Incorporating alternative data into the credit process, on the other hand, can provide stronger digital identities that offer a clearer understanding of who organizations should trust.

PERSONAL PRIVACY: EVOLVING CONSUMER SENTIMENT

There has long been a paradox in online privacy. Based on any survey or report, people state they care about their online privacy and what companies will use with the data that they give. Despite the stance, their online behavior does not reflect that concern. MIT and Stanford researchers measured this very fact, providing four digital wallet options to students with varying levels of detail in the security and privacy of data supplied. Despite concerns about sharing personal information, the order in which the wallets were presented provided the best indication of which wallet the students would select. Going further, the researchers offered students free pizza if they passed along three friends' emails.[11] Again, even those that claimed to have high levels of concern for privacy shared emails due to the incentive of free pizza. Even if there are few bigger draws to a college student than pizza, the incentivized impulse on display in the study has also led to a number of efforts to help people monetize their identities and sell data. But consumers do not know who they are selling to, why, and what will then be done with the data once it is sold.

The Privacy Actives Segment

I care
I care about data privacy
I care about protecting others
I want more control

and

I'm willing to act
I am wiling to spend time and money to protect my data
This is a buying factor for me
I expect to pay more

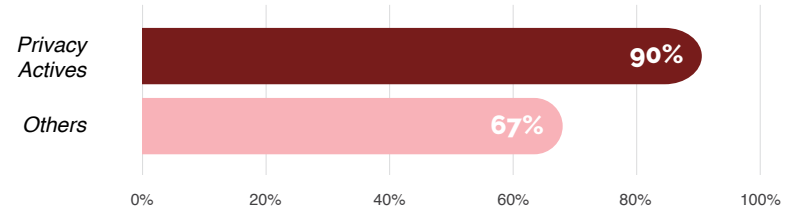
and

I've acted
I have switched companies or providers over their data policies or data sharing practices

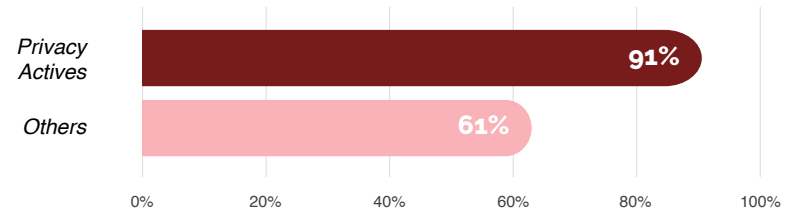
Privacy Actives

Attitudes of Privacy Actives Versus Others

How they treat data is how they treat me



How they treat data is how they treat me



10%
of consumers feel like they have complete control over their personal info and only

25%
of consumers believe most companies handle their sensitive personal data responsibly

25%
of consumers say they fully understand digital identity

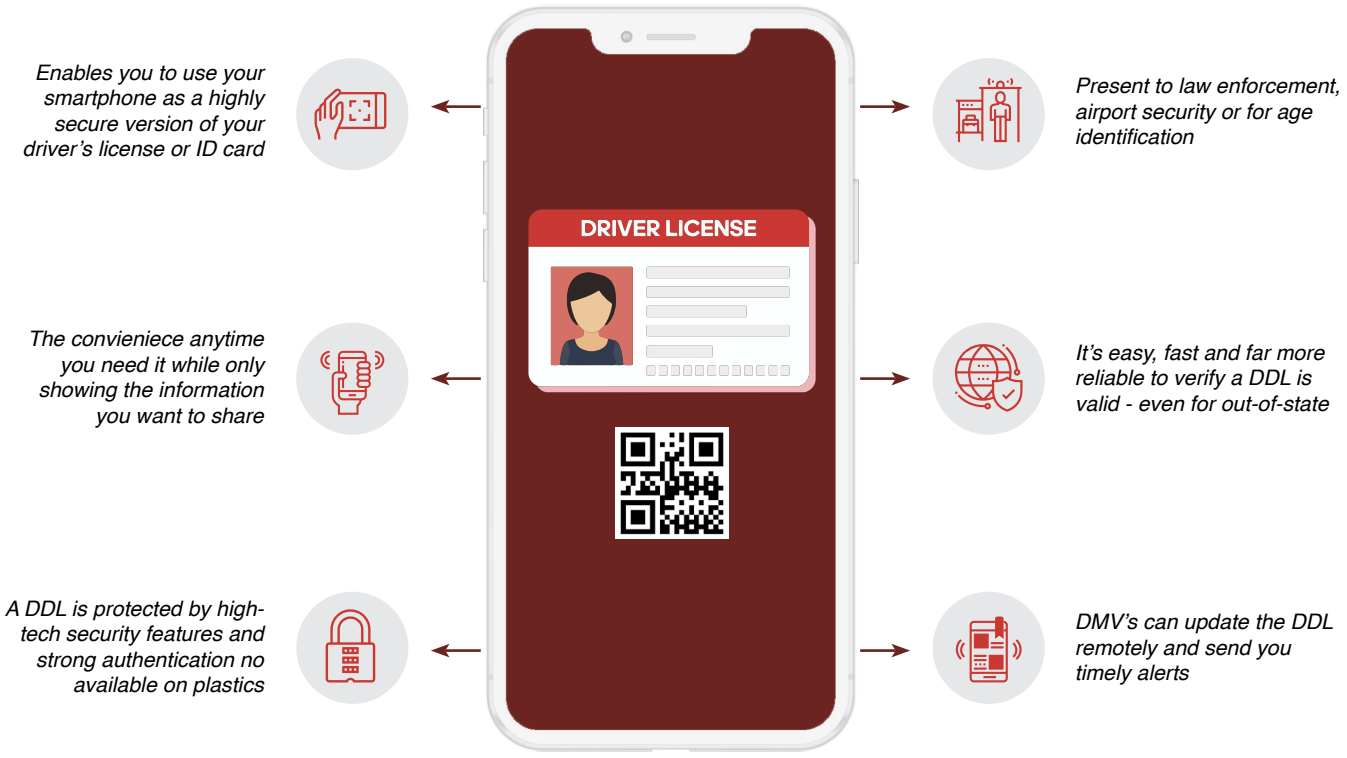
Source: Cisco,[12] Mitek,[13] and PwC[14]

Consumers' online behavior does not align with their stated concerns about digital privacy. Furthermore, consumers have a limited understanding of what digital identity entails. While some may have heard of the term, most equate digital identity to social log-ins for convenient account access across services. While that may be one use, they do not understand how the tools to produce secure digital identities work. They do not understand the nuts and bolts of DI and, therefore, do not grasp the potential. Nor should they need to. They only must understand the reason to confirm the identity, to provide them an understanding of why a company must collect the data it asks for.

Private entities deserve some blame for this educational gap. While there is a constant balance between friction and security, the need to develop easier ways to inform consumers of their rights has often been left to the wayside in favor of less friction. Much of this frictionless design has been to intentionally avoid informing customers of their rights, allowing companies to pull more personalized data. This tactic raised risk measures while changing regulations have forced some pull back of that frictionless experience. Again, while security and a frictionless experience can work as one, it also requires a bit of understanding of the consumer in why they act one way online versus what they say in person. Their decisions indicate that they do not understand what their online actions mean and they value convenience over other matters. To maintain trust, especially as GDPR, CCPA, and other regulations force organizations to be more transparent with customers about why they need certain personal data, companies will differentiate themselves through the transparency they provide in why they seek the information.

Part of this knowledge gap may be due to a lack of personal experience with digital identity, which may be mitigated by efforts like the DMV Modernization Act, which would allow for digital driver's licenses and the normalization of digital IDs across the US. About a dozen states, including California, are currently testing the development of digital licenses.[15] These licenses would offer the ability for users to hold a digital license on their phone, then share either the age, age and photo, address only, or any other piece of information standard on a license. When pulled over by a cop, the officer could scan all the information, as needed. If someone wanted to check out a library book, the librarian could scan the license pulling the name and address and nothing else. If someone needed to apply for a car loan, the bank could pull the address and confirm the license number, without having to access any other piece of personal data.

What is a Mobile or Digital Drivers License (DDL)?



These various day-to-day use cases can increase exposure to digital identity. Such experiences will lead to better understanding of what digital identity can do for consumers, making it easier in the private sector to incorporate more apparent DI designs. Until then, communication and transparency that organizations provide in seeking data matters. Providing that insight through a fluid design, instead of legalese, allows for even further education. Offering onboarding flows that allow for both ease of use and a moment to educate users about what and why a company needs certain data points can help in this transition, as they begin to understand digital identity in greater scope.

CONCLUSION

Organizations must show they care about user privacy, data, and digital identities to produce the most benefits from the technology in order to display proactiveness and transparency. In a simple KYC effort to approve a student for a rental, as an example, a landlord very well may find that the person has been rejected due to a credit risk. Using standard methods, the landlord would then move on to the next potential tenant. Now, with more insight into the KYC and onboarding process, someone with the incentive to do so can look at what led to the rejection. It might have occurred because the person in question has moved around multiple times in the past few years. For a student, however, this should not serve as a disqualifying characteristic since most students move often while in school. By understanding that, the organization can capture an otherwise highly qualified tenant. To do so, however, requires the right tools and a proactive approach.

A comparable issue can rise in all sorts of various sectors. The important aspect is to seek out tools that can provide the oversight. A true solution to the challenges of digital identity and identity verification would require cross-border collaborative efforts by regulators to establish standards and baselines. Companies do not have control of that effort, but the digital identity capabilities to adjust to new borders and regulations while complying to local laws remain. The same holistic approach is vital in fighting the evolving online fraud and crime landscape. Since people, fraud techniques, and identities do not remain static, solutions must move with businesses in order to adapt and correctly authenticate customers, users, or clients. It is that tools and rules mindset. The rules will change, so focus on the tools that provide the most capability to capture the benefits and insights from digital identity and the data collected, and then scale based on how laws and fraud shift, using partners and vendors as resources.

Has the business built in the level of transparency to adapt to changing privacy laws? Has the company found the right vendors and technology tools to adjust as the organization scales and regulations change? The time to find out is now.

ABOUT

KNOW IDENTITY DIGITAL ROUNDTABLES

KNOW Identity Digital Roundtables, presented by One World Identity, convene identity thought leaders, C-Suite executives, and industry operators who are implementing digital identity solutions at scale. Our Digital Roundtable series includes intimate breakout rooms to facilitate live discussion in a closed-door environment, providing our contributors with the opportunity to shape the agenda. Throughout the roundtable, members are encouraged to engage, pose questions, and in some cases, spar with their peers. The goal of the KNOW Identity Digital Roundtable series is to:

- Engage an active community to share ideas, discuss challenges, and determine action plans to bring digital identity solutions to the forefront
- Facilitate thoughtful conversation and allow for cross-industry collaboration

Interested in joining our elite group of senior executives, changemakers, subject matter experts, and investors? Check out our lineup of upcoming events.

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.

TRULIOO

Trulioo, a leading global identity and business verification company, provides instant identity and business verification for 5 billion people and 330 million companies worldwide.

Founded in 2011 by Stephen Ufford and Tanis Jorge, Trulioo is based in Vancouver, Canada with an office in Dublin and team members located throughout the U.S.

Our mission is focused around three principles: trust, privacy and inclusion. Our team is dedicated to building a framework of trust and safety online, developing best privacy practices and advancing financial inclusion. These principles are enabled by our bank-grade global identity and business verification platform, Trulioo GlobalGateway.

As a pioneer in the identity space, Trulioo has developed a client base that spans the globe — ranging from large financial institutions to innovative tech companies. We optimize our technology and global data partnerships in order to help our clients scale their Customer Due Diligence (CDD), Know Your Customer (KYC) and Anti-Money Laundering (AML) operations into new markets faster, more efficiently and at a reduced cost.

CONTRIBUTORS

15MB LTD., DAVE BIRCH, PRINCIPAL

AIRBNB, ADEL SABIROVA, DATA SCIENCE LEADER

AVAST, ANTON LEGH, STRATEGY DIRECTOR

AWS, SCOTT SHEPHERD, GLOBAL PRINCIPAL IDENTITY SPECIALIST

ACXIOM, SCARLETT BURKS, DIRECTOR OF DATA/IDENTITY MARKETING

CAPITAL ONE, PRANAV KHANNA, VP

CLARITAS, AL GADBUT, CTO

CLARITAS, LUCIANA SOBOCINSK, VP, STRATEGY & MEASUREMENT

CUSTOMS & BORDER PROTECTION, TRACY MINTER, PROGRAM MANAGER

EARLY WARNING SERVICES, CARLO CAPELLO, DIRECTOR, PRODUCT AND BUSINESS DEVELOPMENT

ENSTREAM, JANICE MASOTTI, CMO

FEDERAL RESERVE BANK OF BOSTON, RUDIE LION, INDUSTRY CONSULTANT

FIDELITY INVESTMENTS, ROBIN WEISS, SENIOR TECHNOLOGY ADVISOR

FRIDAY, HUE RHODES, CEO

FULLCONTACT, CHRISTOPHER HARRISON, CEO

HD CONSULTING, JIM KRAGH, COMPLIANCE CONSULTANT

IDMISSION, ALEX RUSCHIN, SENIOR EXECUTIVE PARTNERSHIPS

IHS MARKIT, CHERYL GOODNOW, HEAD OF STRATEGIC ALLIANCES, PLATFORMS & REGULATORY COMPLIANCE

INE, ALEJANDRO ANDRADE, COORDINADOR DE PROCESOS TECNOLÓGICOS

IPROOV, JOE PALMER, PRESIDENT

JEFFERIES, ERIK NELSON, SENIOR VICE PRESIDENT

JOURNEY.AI, JULIE RUNDA, VP CONTENT MARKETING

JOURNEY.AI, MARK BAKIES, VP OF PRODUCT MANAGEMENT

JPMORGAN CHASE, YAN YANG, PRODUCT MANAGER

KIBS.MK, MARIN PIPERKOSKI, CEO ADVISOR

LIVELY, CATHERINE GAVIN, COMPLIANCE COUNSEL

LIVE NATION (TICKETMASTER), PAUL KUYKENDALL, FORMER VP, PRODUCT GLOBAL PAYMENTS

LYFT, SHIVENDRA KISHOR, HEAD OF FRAUD, IDENTITY & ABUSE - ANALYTICS & OPERATION

MASTERCARD, MARCELO BELLINI GARCIA, VICE PRESIDENT, PRODUCT MANAGEMENT, DIGITAL IDENTITY

MASTERCARD, DENNIS GAMIELLO, SVP, IDENTITY SOLUTIONS

NTTDATA, SHEUECHEE BEH, SENIOR MANAGER

OCR SOLUTIONS, EYAL BARSKY, PRESIDENT/CEO

PARKWOOD ADVISORS LLC, JOHN PARKINSON, MANAGING DIRECTOR

PAYONEER, RAN DANIEL, PROJECT MANAGER

PAYONEER, MOSHE SHEVEL, OPERATIONS AND SERVICES KNOWLEDGE EXPERT

PONTIFICAL CATHOLIC UNIVERSITY OF PERU, FLAVIO RODRIGUEZ, TECH ADVISOR

POSHMARK, LAUREN WHITE, ACCOUNT SECURITY MANAGER

POSHMARK, MELANIE QUEIROZ, SENIOR FRAUD MANAGER

REPYUTE NETWORKS PRIVATE LIMITED, DEEPAK DHAR, CEO

SAS, KATIE DEGRAFF, GLOBAL TEAM LEAD - FRAUD & SI

SAS INSTITUTE INC., DIANA ROTHFUSS, SR. GLOBAL PRODUCT MARKETING MGR

SEDICII, ROB LESLIE, CEO

SIMPLE FINANCE, BRIANNA BEYROUTI, MANAGER OF FRAUD OPERATIONS

SPOKEO, HARRISON TANG, CEO

STANCHART, EUGENIA KARIKARI, DIGITAL CLIENT SERVICE EXECUTIVE

SUSTANY CAPITAL, CHRISTIAN KAMEIR, MANAGING PARTNER

TRANSUNION, JEFF JOHNSTON, FRAUD AND IDENTITY ADVISOR

TRANSUNION, CHAD GLUFF, DIRECTOR - FRAUD & IDENTITY

TRULIOO, IVAN YANG, STRATEGIC ACCOUNT EXECUTIVE

TRULIOO, LUCY SCRENCI, SENIOR PR AND COMMUNICATIONS MANAGER.

US BANK, MORRIS JACKSON, SVP, MARKET LEADER

ENDNOTES

1. “CCPA Identity Verification Compliance: Trial & Error,” Evident ID, https://www.evidentid.com/resources/ccpa-identity-verification-compliance-trial-error/

2. “Consumer Privacy Report - Cisco Cybersecurity Series Feb 2020,” Cisco, https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf

3. “Facilitating Trust in a Shifting Identity Landscape,” Trulioo & OWI, https://oneworldidentity.com/reports/facilitating-trust-trulioo/

4. “Fintech, Regtech And The Role Of Compliance In 2019 Part 4: Industry Opinion, Challenges For Firms, Cyber Resilience, Closing Thoughts,” JD Supra, https://www.jdsupra.com/legalnews/fintech-regtech-and-the-role-of-76911/

5. “Beware of Robocalls, Texts and Emails Promising COVID-19 Cures or Stimulus Payments,” AARP, https://www.aarp.org/money/scams-fraud/info-2020/coronavirus.html

6. “Holiday Fraud Concerns During Pandemic Come True,” Transunion, https://newsroom.transunion.com/holiday-fraud-concerns-during-pandemic-come-true/

7. “Holiday Fraud Concerns During Pandemic Come True,” Transunion, https://newsroom.transunion.com/holiday-fraud-concerns-during-pandemic-come-true/

8. “Consumers trust your tech even less than you think,” PwC, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/trusted-tech.html

9. “The Power of First Impressions Online,” Trulioo, https://id.trulioo.com/rs/392-YOD-077/images/Trulioo-industry-report-AccountOpening2020.pdf

10. “Addition Is Better Than Subtraction,” PERC, https://www.perc.net/wp-content/uploads/2020/06/credit-data-suppression-deletion-addition.pdf

11. “Pizza over privacy? Stanford economist examines a paradox of the digital age,” Stanford University, https://news.stanford.edu/2017/08/03/pizza-privacy-stanford-economist-examines-paradox-digital-age/

12. “Consumer Privacy Report - Cisco Cybersecurity Series Feb 2020,” Cisco, https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf

13. “Digital identity 2020: Drivers and challenges,” Mitek, https://www.miteksystems.com/innovation-hub/research-reports/digital-identity-2020-drivers-and-challenges#cover

14. “How consumers see cybersecurity and privacy risks and what to do about it,” PwC, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html

15. “Upgrading your wallet: How soon can I get a digital driver’s license?,” USA Today, https://www.usatoday.com/story/tech/2019/03/06/how-soon-can-get-digital-drivers-license/3072888002/