docusign | ENTRUST SECURING A WORLD IN MOTION

Whitepaper

The Future of Global Identity Verification

How leading organizations balance digital security with user experience

As incidents of identity fraud become more commonplace, organizations around the world are seeking new ways to verify and authenticate their customers' identities. Identity verification (IDV) and authentication solutions provide this crucial layer of security. With greater insight into how leading organizations deploy these solutions, and awareness of the most vulnerable areas of the customer journey, businesses can better protect themselves from increasing risks.

Docusign and Onfido, an Entrust company, co-created this report to understand the state of identity fraud around the world and the role IDV plays in addressing it. Along with providing a macro global perspective on where identity fraud occurs in the customer journey and how teams are responding to the growing threat, the research reveals the specific challenges faced by organizations on a regional and industry level.

Key findings

1 **Identity fraud incidents are on the rise, costing organizations time, money, and employee resources.**

A significant portion of organizations surveyed lose over $1 million each year to direct and indirect identity fraud-related costs—and these expenses will likely rise as artificial intelligence (AI) advances. Despite the challenges, some organizations are hesitant to implement identity fraud prevention solutions out of fear they will add friction to the customer experience. Sixty-six percent of organizations surveyed agree that customer experience and identity fraud prevention are competing priorities. However, in practice, many businesses find that they don't have to compromise: Businesses that use IDV are twice as satisfied as businesses that do not use IDV.

2 **Identity fraud takes place throughout the customer journey, but it most often occurs when customers log in and authorize payment.**

Along with seeing identity fraud at various stages of the customer journey, businesses see many varieties. The most common forms across industries are identity theft, account creation, digital document forgery, and chargeback fraud. The authentication method linked with the most identity fraud is username and password. A deeper dive into organizational behavior reveals that two-thirds of organizations apply different levels of authentication for each customer interaction, based on either their customers' risk profiles or the type of interaction.

3 **IDV is not only a powerful line of defense for organizations in preventing identity fraud but can also result in a competitive advantage.**

IDV users detect identity fraud earlier in the customer journey and more frequently than non-users. As a result, the average organization using IDV has saved over $8 million in total by preventing identity fraud with an IDV solution. Sixty-three percent of organizations that invested significantly more in IDV than their industry peers believe the steps they took to prevent identity fraud had a positive impact on their brand.

4 **Most organizations see technology as the solution to solving or mitigating customer fraud.**

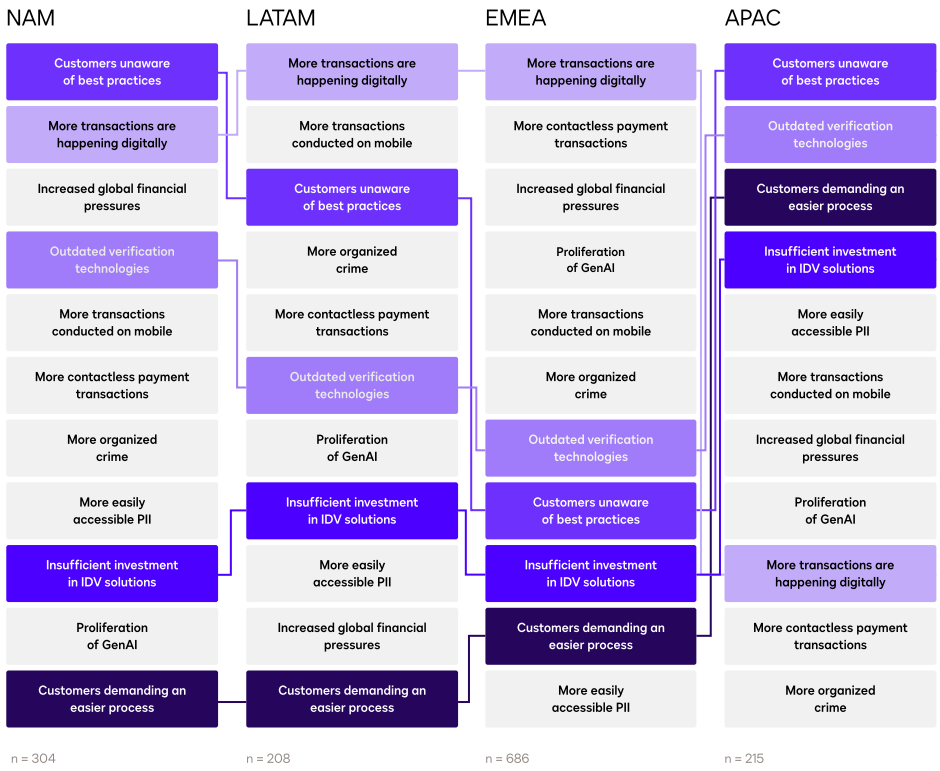
Seventy percent of organizations surveyed believe investing heavily in technology solutions is the best way to mitigate the financial risk of identity fraud, and IDV is one of their top priorities, with 74% planning to invest more in IDV in the future.

Identity fraud is a growing concern, along with high costs and rising customer expectations

Sixty-nine percent of organizations surveyed agree: Identity fraud attempts are on the rise. While the majority of businesses across the globe share this challenge, their beliefs about what's driving the uptick differ across industry and region. However, two reasons rose to the top of our research:

- More digital transactions are taking place today
- Customers are not familiar with best practices to protect their login information and other sensitive data

Lack of customer awareness on best practices and a rise in digital transactions lead reasons for increased fraud attempts



What do you believe are the biggest reasons why there's been an increase in fraud attempts?

Although few organizations selected AI as a leading driver of fraud in this survey, other research indicates it may heavily contribute to the changing security landscape. Entrust's 2025 Identity Fraud Report found that digital document forgeries, often created with generative AI, **increased 244% in the past year.** Deepfakes like these forgeries now account for 40% of all biometric fraud. At the same time, many businesses see AI as a critical tool to combat identity fraud: 82% of respondents believe generative AI will be more effective than their current methods at reducing customer fraud risk.

There are also patterns in the varieties of identity fraud organizations observed. Across industries, identity theft was the most commonly reported identity fraud, followed by digital document forgery and account creation fraud. Retail and e-commerce are the only industries with another type of fraud in their top three: chargeback fraud (when customers intentionally dispute a charge to receive a refund while keeping the product or service). This is due to the role of consumer purchases in this industry.

These findings show that most identity fraud occurs at critical identity moments when customers actively engage with a business, whether creating an account for the first time, resetting their password, or entering payment information. To protect these critical moments in the customer journey, businesses need to offer ways to safely open accounts and continually verify users' identities throughout the customer lifecycle.

Identity theft, account creation, and digital document forgeries lead as most common types of identity fraud across industries

What types of fraud related to identity verification/user authentication are most common for your organization in the customer transaction process?

Regional findings

Brazil respondents reported the highest increase in identity fraud attempts out of countries surveyed, with

79%

of organizations reporting a rise in fraud.

Percentage of organizations with direct identity fraud costs over $1 million

Countries with highest percentage

55% Germany
65% Australia

Countries with lowest percentage

30% United Kingdom
29% Brazil

Percentage of organizations with indirect identity fraud costs over $1 million

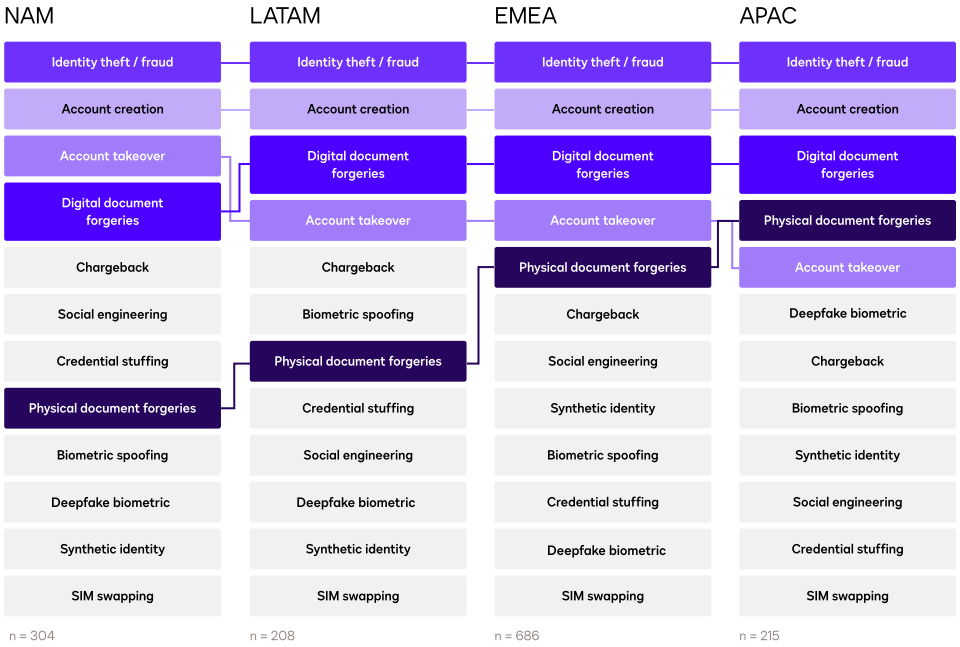
Countries with highest percentage

24% Brazil
29% Australia

Countries with lowest percentage

6% Mexico

Identity theft, account creation, and digital document forgeries lead as most common types of identity fraud across regions



What types of fraud related to identity verification/user authentication are most common for your organization in the customer transaction process? Please click to rank up to 3 that happen regularly, starting with the most frequent.

Industry findings

The banking and finance industry reported the highest direct identity fraud costs. (51% reported annual direct costs over $1M)

The professional services industry reported the highest indirect identity fraud costs. (20% reported annual indirect costs over $1M)

Identity fraud costs organizations an average of $7 million per year

Many organizations believe the costs associated with identity fraud are simply the price of doing business, but that price is rising each day. Organizations regularly face expenses over seven figures due to the direct costs of chargebacks, refunds, and other financial losses and the indirect costs associated with dedicating valuable employee resources to identify and remedy fraudulent transactions and address brand and reputational damage. Our research revealed that:

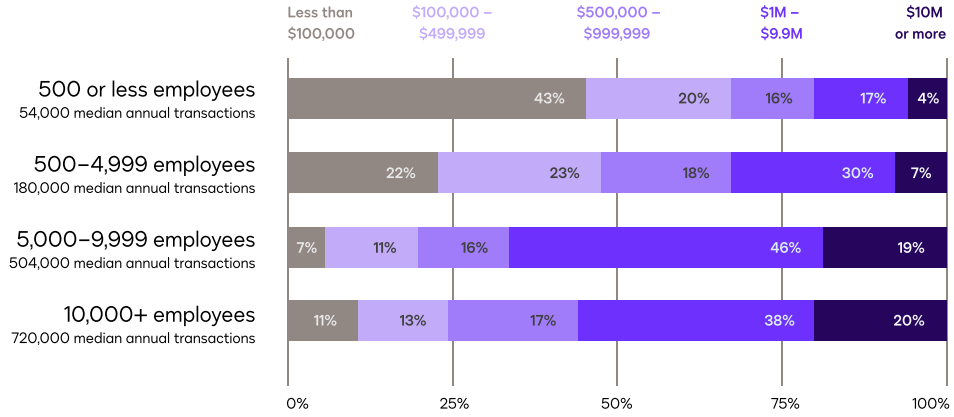
41%
of organizations have an annual direct identity fraud cost over $1 million.

15%
of organizations have an annual indirect identity fraud cost over $1 million.

Larger organizations—which handle more customers, data, and revenue—see even higher costs.

- **Organizations with over 5,000 employees have an annual direct identity fraud cost of $13 million on average.** Additionally, 28% of these organizations have an annual indirect identity fraud cost over $1 million.
- And the costs grow by multiples as the size of organizations increase. **Among organizations with over 10,000 employees, 20% have annual direct and indirect identity fraud costs over $50 million.**

Large organizations see higher direct identity fraud costs



If you had to estimate, what is the approximate annual direct financial cost of customer fraud for your organization? By direct financial cost, we mean the amount of money lost because of fraud, regardless of whether you're compensated by insurance.

At the industry level, banking and finance face the highest direct costs of identity fraud. This is because fraudsters create fake accounts at the customer onboarding stage, which allows them access to monetary services, or gain access to legitimate accounts during a later stage of the customer lifecycle and drain them of funds. In both scenarios, the targeted business loses money directly or has to pay back the genuine customer.

The professional services industry sees the highest indirect costs of identity fraud. Identity fraud is more likely to affect these businesses' brand reputations and customer trust, which drives away future revenue and results in significant indirect costs.

Customers increasingly expect frictionless experiences

66%
of organizations surveyed believe customer experience and identity fraud prevention are competing priorities.

45%
of organizations surveyed prioritize customer experience over fraud prevention.

58%
of organizations surveyed are concerned they will frustrate customers and increase abandonment rates if they increase identity fraud prevention.

79% of organizations surveyed agree that customer experience is very important to their success.

Businesses are under pressure to deliver easy, convenient, and competitive digital experiences while also keeping customer information secure. For instance, many customers expect personalized experiences, mobile-friendly transactions, and pre-populated forms with information they've already provided, but they also assume their data will remain safe throughout these interactions. Many organizations struggle to balance these aims.

However, approaches to balancing identity fraud prevention and customer experience vary across regions, industries, and generations. The IT and banking and finance industries are more likely to put customers through intense authentication measures to protect confidential data and high-value transactions, respectively, even when the measures create more friction.

Millennial and Gen Z decision-makers, who are more accustomed to digital identity verification checks, expect exceptional user experiences and security during digital transactions—and are driving tech innovation as a result.

Overall, businesses that use IDV are 2x more satisfied with this method than businesses that do not use IDV, and tend to find their fraud prevention methods significantly more effective.

Regional findings

APAC is even more concerned about the friction between customer experience and identity fraud prevention, with

80%
of organizations agreeing they are competing priorities.

Key takeaway

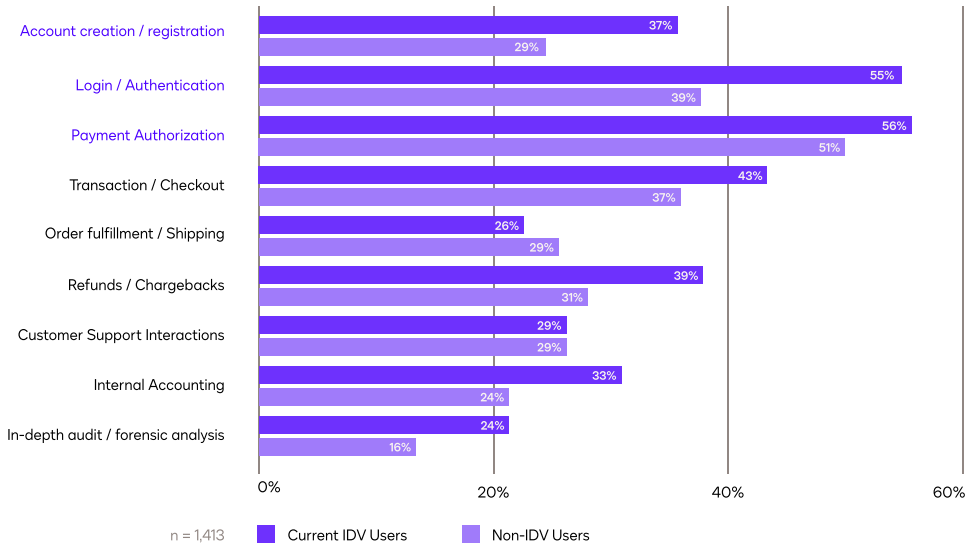
Managing increasing identity fraud attempts while delivering a frictionless experience is a growing challenge, but IDV helps organizations reduce identity fraud while delivering greater organizational satisfaction. Businesses that use outdated or insufficient technologies to mitigate the risk of identity fraud will struggle to defend against complex identity fraud techniques or keep pace with new threats.

Identity fraud occurs throughout the customer journey

Identity fraud occurs throughout the customer journey, but organizations **most often detect it at the early stages of login and payment authorization.**

Organizations that use IDV are even more likely to learn about identity fraud attempts early during transactions, improving their chances of preventing or mitigating damage.

IDV users are more likely than non-users to discover fraud at early stages of customer journey



At what point in the transaction process does your organization typically learn that a fraudulent transaction has occurred? The options listed below are in descending order from initial customer interactions to post-customer engagement processing.

When asked which authentication tools are associated with the most identity fraud, businesses selected **username and password authentication as the most common method**. This could be because usernames and passwords are easily compromised, prone to data breaches, and lack multi-factor authentication. In 2024, stolen credentials like username and password were the most common source of data breach incidents.[1]

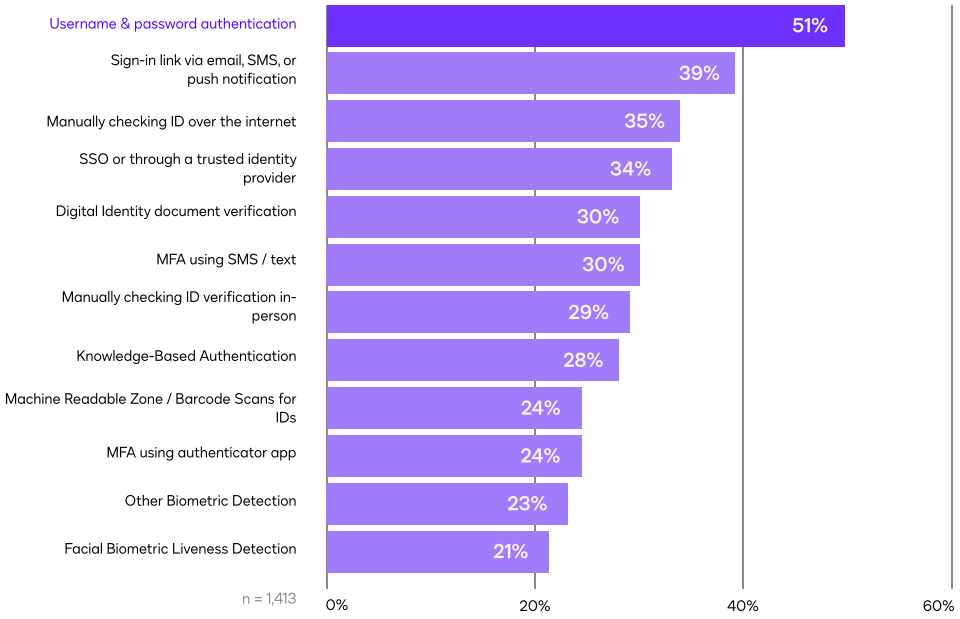
1 "2024 Data Breach Investigations Report," Verizon Business.

Organizations that use IDV, on average, catch identity fraud attempts in

20%

more stages of the customer journey than non-users.

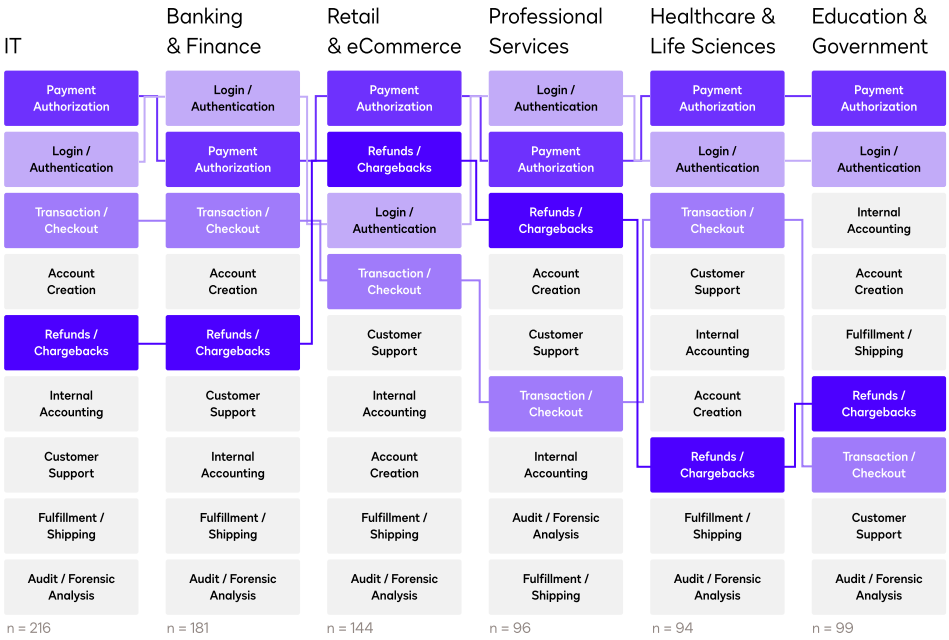
Identity fraud occurs most when username and password alone is the authentication method



For each type of user authentication, please indicate whether fraud is more common with this technique.

The survey also revealed that the more digital transactions an organization handles, the greater the likelihood of them finding fraud across a variety of authentication methods.

Payment authorization and login are the most common stages to discover fraud across industries

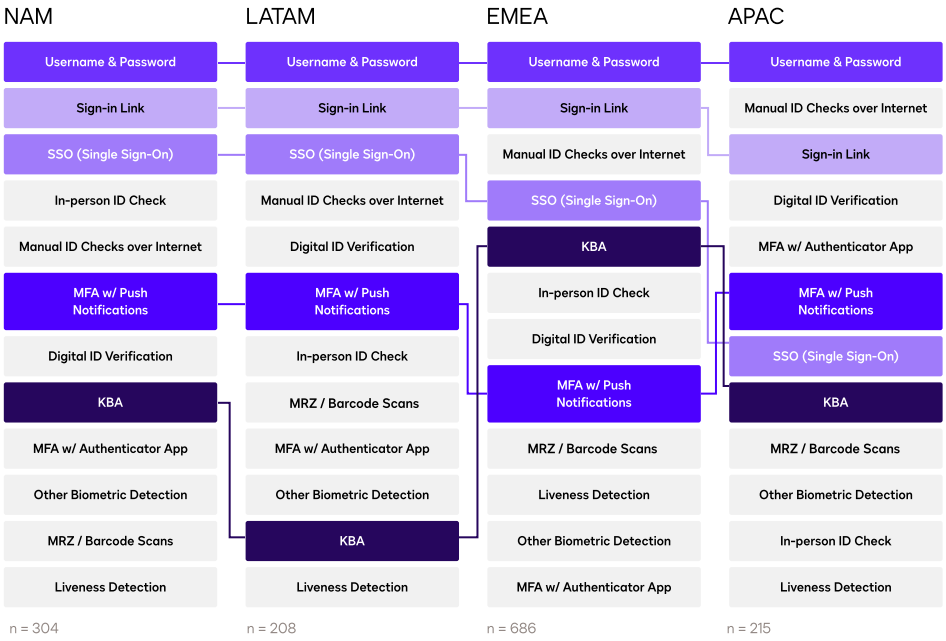


At what points in the transaction process does your organization learn that a fraudulent transaction has occurred?

Generational findings

Among IT and business decision-makers, millennial and Gen Z leaders are more likely to use IDV than baby boomers or Gen X. They are also more likely to rate their organization as "very good" in their anti-fraud approach.

Username and password is the authentication method associated with the most fraud across regions



Fraud is much more common than average with this technique.

Key takeaway

Username and password is the most vulnerable authentication method, but even MFA isn't sufficient to protect against increasingly complicated identity fraud attempts. Advanced forms of IDV like biometric authentication and document verification are essential to stay ahead of fraudsters.

Significant investment in IDV has real results

The average organization has saved more than

$8 million

in total by preventing fraud with an IDV solution.

But deploying an IDV solution is only the first step. Businesses that see the greatest results place intense focus on their security by investing significantly more than their peers in IDV. Additionally, businesses that invest more make their organization a less attractive target to fraudsters, creating a competitive advantage.

Organizations that report investing significantly more than their peers in IDV:

Save more

1.5x

more likely to have saved over $1 million in total than those who invested somewhat more than their peers.

2.2x

more likely to have saved over $1 million in total than those who invested the same or less than their peers.

Have greater internal and customer satisfaction

4x

more likely to be very satisfied with the IDV solutions they use.

1.6x

more likely to have had a positive impact on their brand.

Lower the amount of identity fraud

1.7x

more likely to have successfully reduced a significant amount of identity fraud.

Are more competitive

2.7x

more likely to believe they have a competitive advantage.

Continue to invest in IDV

2.8x

more likely to plan to invest more in IDV.

The data implies customers place more trust in businesses that go above and beyond to protect their personal data.

77%

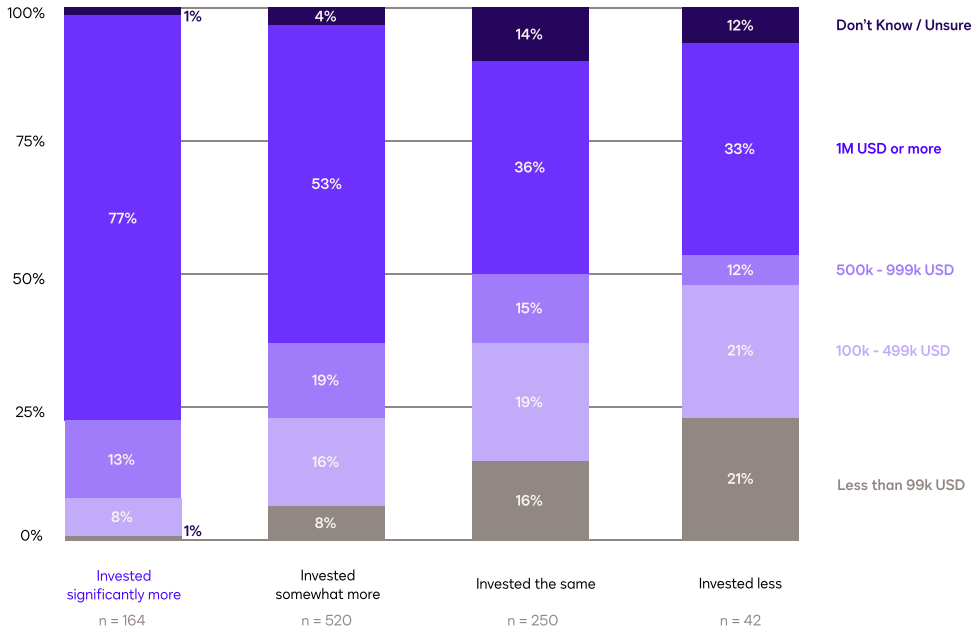
of organizations that invested significantly more in identity verification technologies than their peers have

saved over $1 million

in total, compared to 36% that invested the same as their peers.

Organizations that invested significantly more than peers in IDV were more likely to save a total of $1 million or more

Money Saved With Current IDV Solutions



If you had to estimate, approximately how much money has your organization saved by preventing customer fraud by using your current ID verification/user authentication solutions?

Large organizations invest more in IDV, and realize disproportionately greater return on investment (ROI)

For businesses experiencing a considerable amount of identity fraud, investing in IDV leads to increased ROI. The data show that large organizations, which see higher identity fraud costs, tend to invest significantly more in IDV solutions than their peers and also reap disproportionately greater ROI as a result.

78%

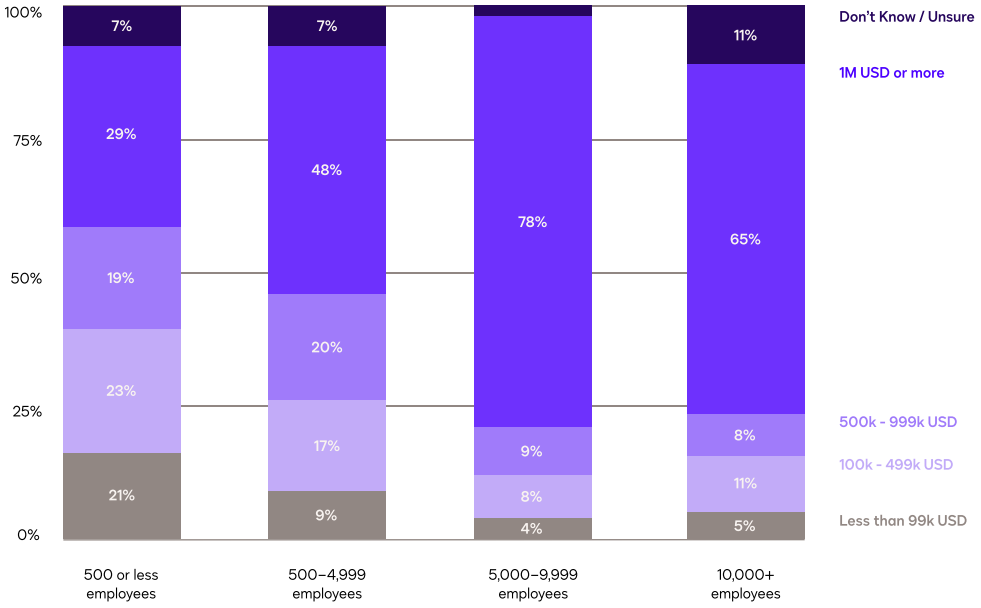
of organizations with 5,000-9,999 employees saved a total of $1 million or more with IDV.

65%

of organizations with over 10,000 employees saved a total of $1 million or more with IDV.

Large organizations save more with IDV solutions

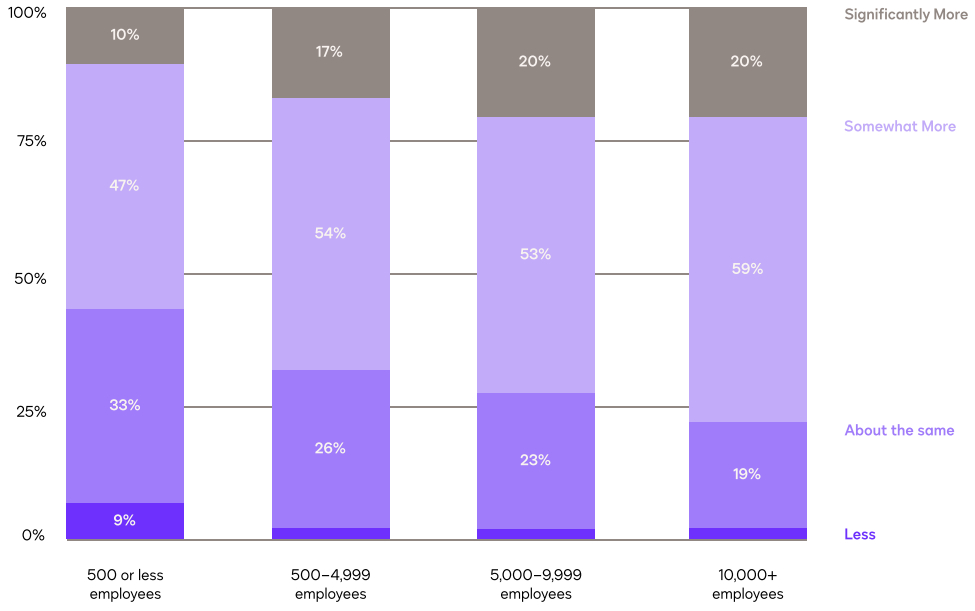
Money Saved Amongst Current IDV Users



If you had to estimate, approximately how much money has your organization saved by preventing customer fraud by using your current ID verification / user authentication solutions?

Large organizations invest significantly more than their industry peers in IDV

IDV Investment Compared to Industry Peers



Which of the following best describes your organization's current investment in ID verification/user authentication solutions/methods?

Key takeaway

Organizations that significantly invest in IDV see a range of benefits, including greater savings, fewer identity fraud incidents, better brand perception, improved customer experiences, and a competitive advantage over peers.

Leading organizations turn toward technology to address fraud

There's a divide in how confident businesses are in their ability to manage identity fraud. 53% think they can mitigate fraud but never completely solve it, while 40% believe they can completely solve it with the right technology. Large organizations with over 10,000 employees tend to fall into the mitigation camp.

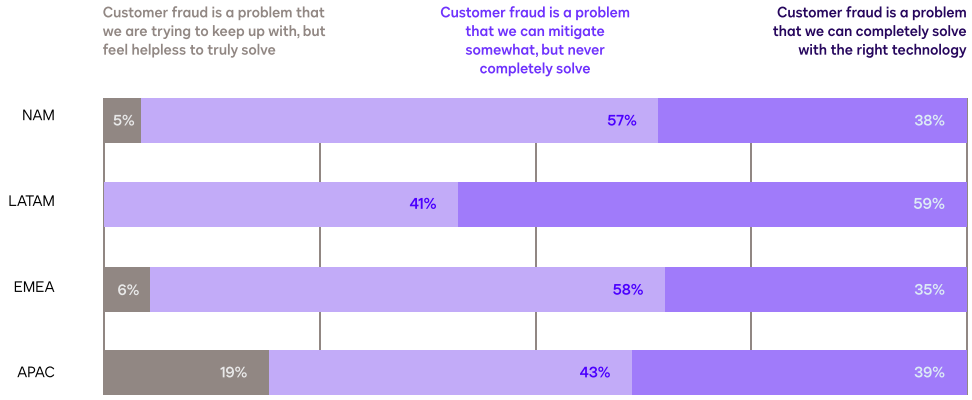
While perceptions differ about the issue itself, most organizations are aligned on a solution:

70%

agree that the best way to mitigate the financial risk of identity fraud is by heavily investing in technology.

Investment in technology overshadows other approaches, such as investing in staff and talent (18%) and investing in business crime insurance to offset fraud costs (11%), reactive options that seek to repair damage rather than proactively defend their organizations from threats.

LATAM organizations are most optimistic about completely solving fraud



Which of the following statements would you agree with more?

Generational findings

Organizational leaders who are millennials and Gen Z are more likely than baby boomers or Gen X to believe fraud can be completely solved with the right technology.

The most popular IDV tool is multi-factor authentication

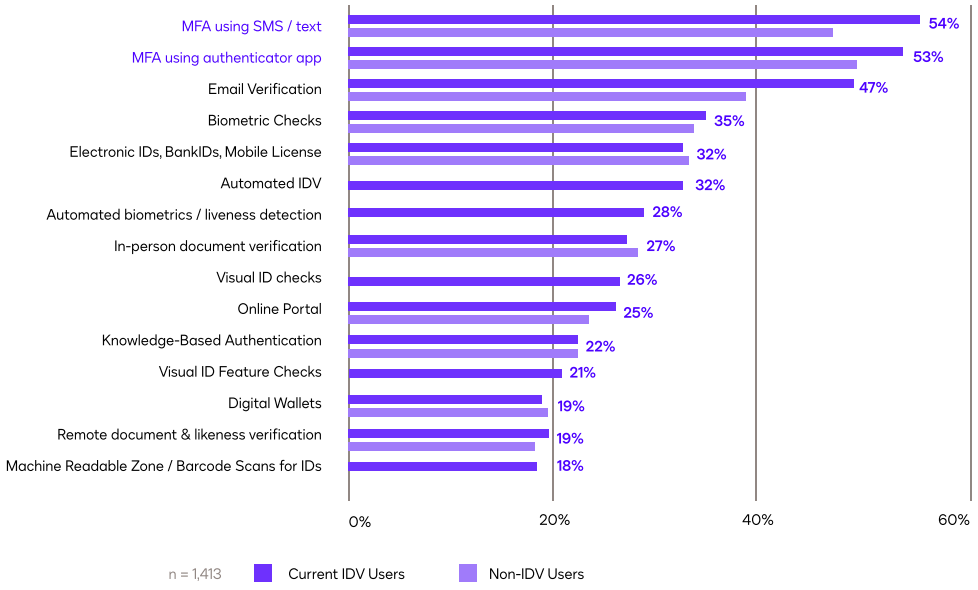
Organizations use IDV tools at a number of different touchpoints in the customer journey, but the most common stage is at username and password authentication—the stage where organizations report the greatest amount of fraud.

Multi-factor authentication (MFA) is the most common tool used by organizations to verify and authenticate identities, whether through SMS and text or with an authentication app.

MFA's popularity is justified: it is one of the oldest methods of digital identification, and customers are accustomed to it, reducing friction for users while providing an essential layer of security.

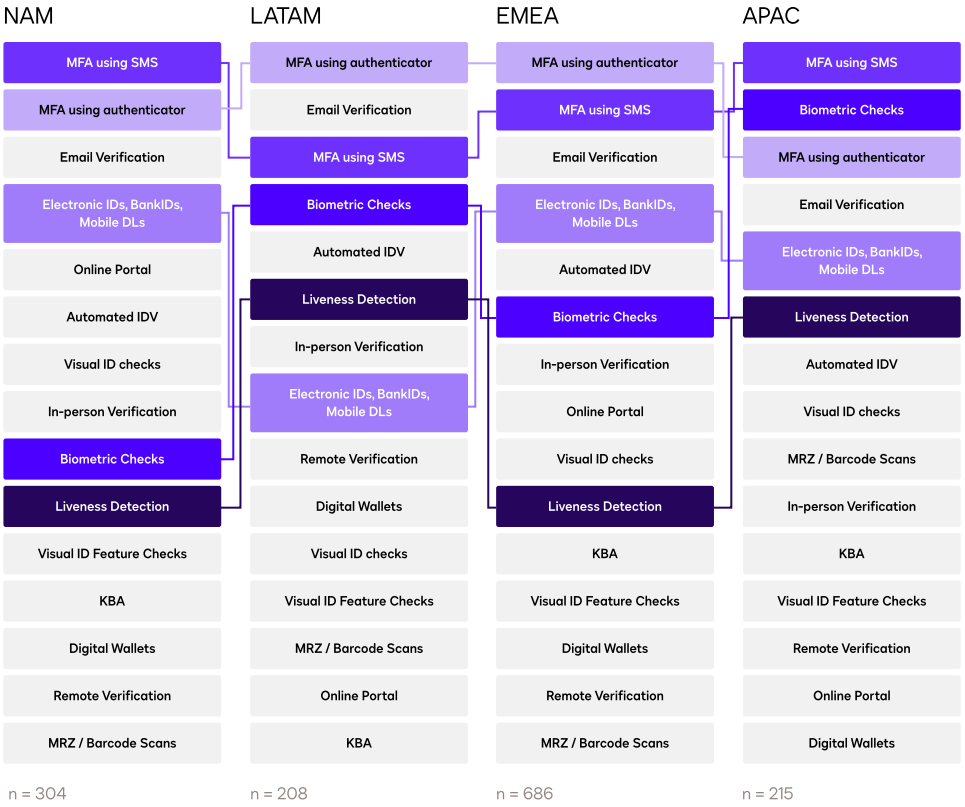
MFA is most common identity verification and authentication tool

Types of IDV and User Authentication Currently Used



Which of the following types of identity verification / user authentication does your organization currently use? Please select all that apply.

Biometric checks more commonly used in APAC; email verification more commonly used in LATAM



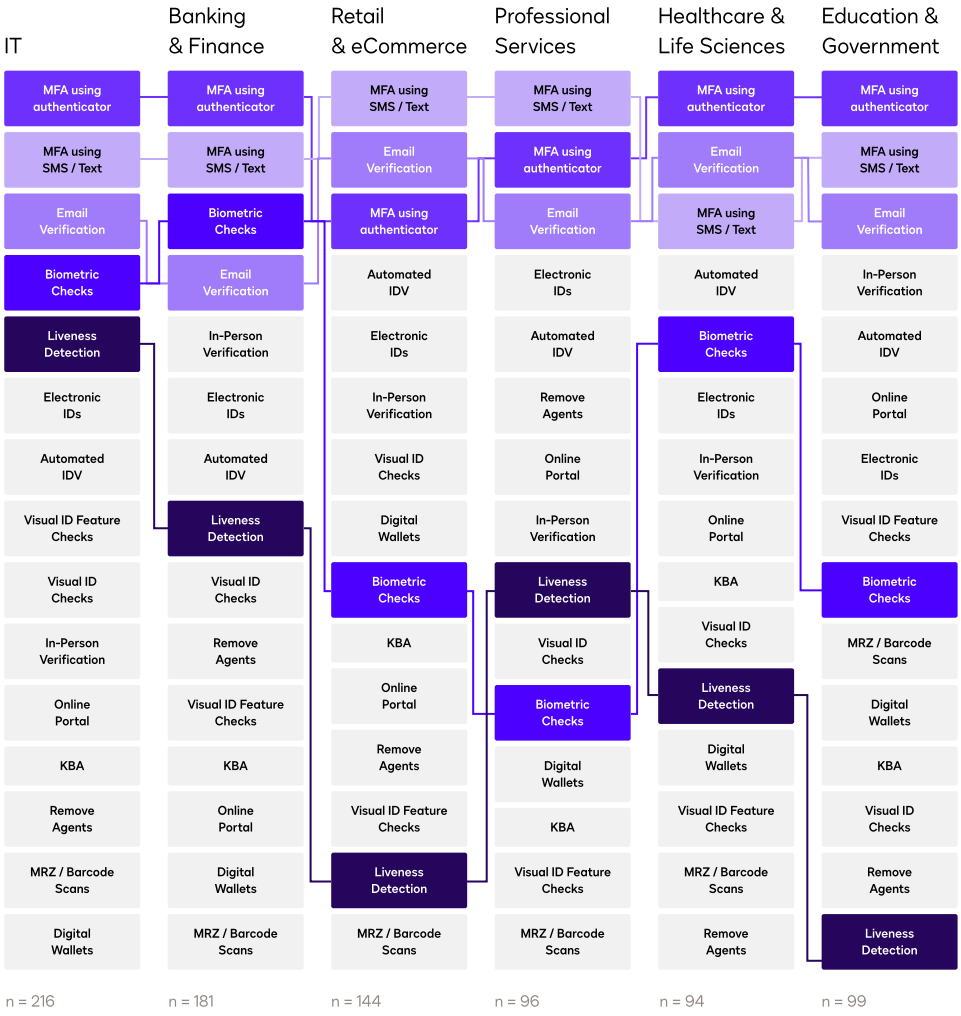
Which of the following types of identity verification / user authentication does your organization currently use?

Decision-makers in France and Germany embrace biometric tools at a lower rate than decision-makers in the UK and other regions.

Generational findings

Organizational leaders who are millennials or Gen Z believe biometrics are an important part of online authentication. According to research from IDEX Biometrics, 47% of this demographic used biometric security methods in the past month. Out of that group, 52% prefer biometric authentication to other methods.

Banking/finance and IT are most likely industries to use biometric checks

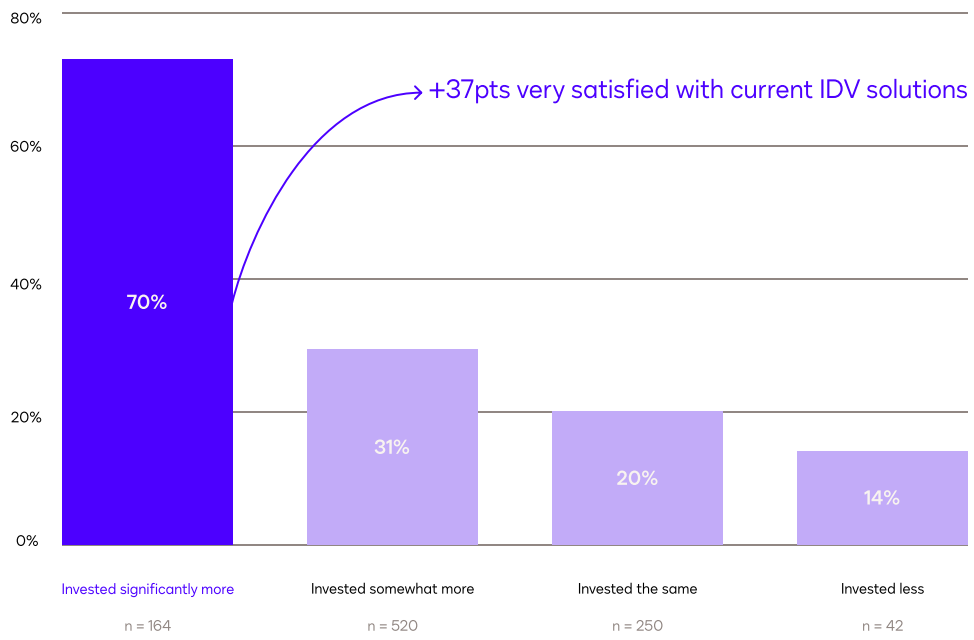


Which of the following types of identity verification / user authentication does your organization currently use?

Businesses that invest more in IDV report higher satisfaction with IDV tools

While MFA is the most common tool, higher investment organizations differentiate themselves by pursuing additional measures. For example, high investors are more likely to deploy sophisticated tools like biometric checks and visual ID features at the sign-in point. This additional effort is linked to greater customer satisfaction with IDV solutions.

Larger investment in IDV compared to peers is linked to higher satisfaction



How satisfied is your organization with the ID verification / user authentication you currently use?

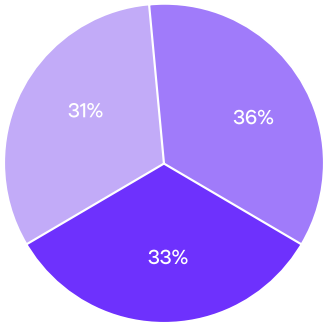
80%

of organizations are willing to put customers through intense levels of authentication, even if they add friction.

Organizations use a variety of methods to determine the appropriate level of authentication for each customer

More than two in three organizations currently use authentication leveling in their security processes. In other words, an organization may implement additional means of authentication for customers who are deemed high risk due to factors like their IP address, distance from sender, or country. They may also implement additional measures for specific types of customer interactions, like opening a new account or accessing finances.

Majority of organizations alter authentication levels for each transaction based on risk profile of customer or type of customer request



Authentication Leveling

- **36%** We use different levels of authentication depending on what type of interaction / request customers are completing
- **31%** We use different levels of authentication depending on a calculated risk profile of the customer
- **33%** We manage all digital identity challenge interactions with customers with the same level of authentication

Which of the following statements best describes how your organization handles fraud prevention?

Organizations use a range of criteria to determine the appropriate level of authentication for each customer interaction, and 62% say choosing the appropriate level is difficult. Businesses most often refer to internal policies and customer risk profiles, but they view **transaction value and cost-benefit analysis as the most important criteria** for assessing risk.

62%
say finding the appropriate level is difficult.

Regional findings

Regulatory requirements are the most common driver for determining authentication levels in the U.S. (17%). They are also more commonly used in Canada (20%) and France (16%) than in other countries.

Industry findings

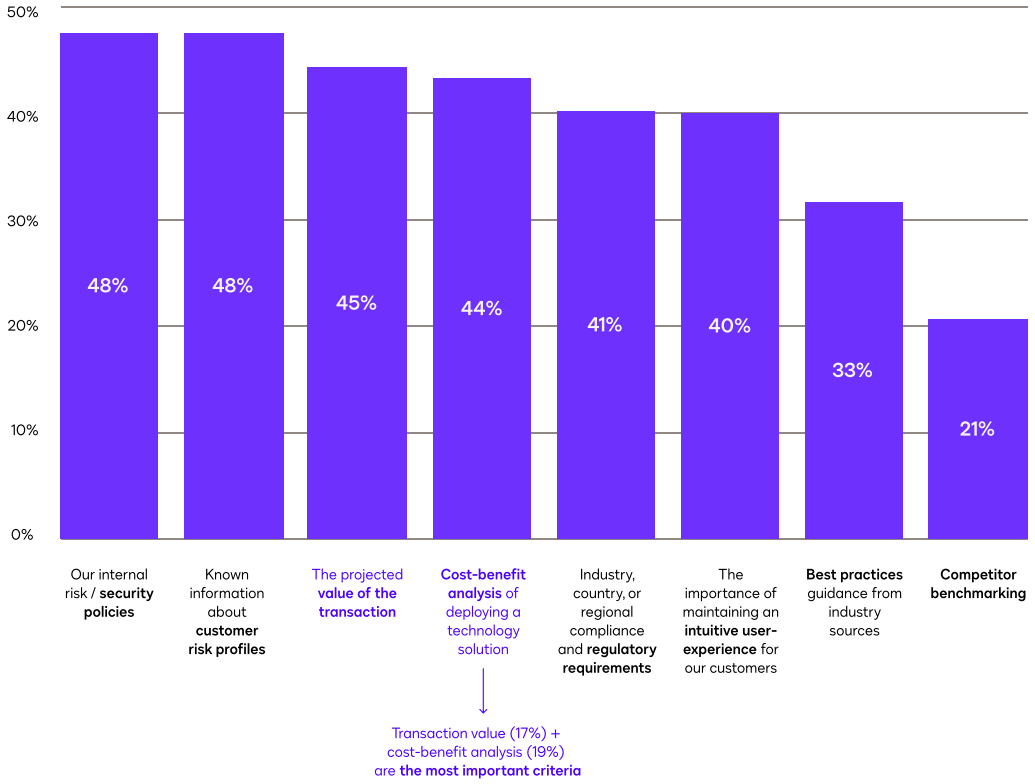
Regulatory requirements are the most popular method for determining authentication levels in the healthcare industry (29%). They are also more commonly used in real estate (25%) and banking and finance (20%) than in other industries.

Internal policies and customer risk profiles are most common methods for determining authentication level

Value of transaction and cost-benefit analysis are considered most important

How do you decide the appropriate level?

Most Used Methods for Determining Authentication Level

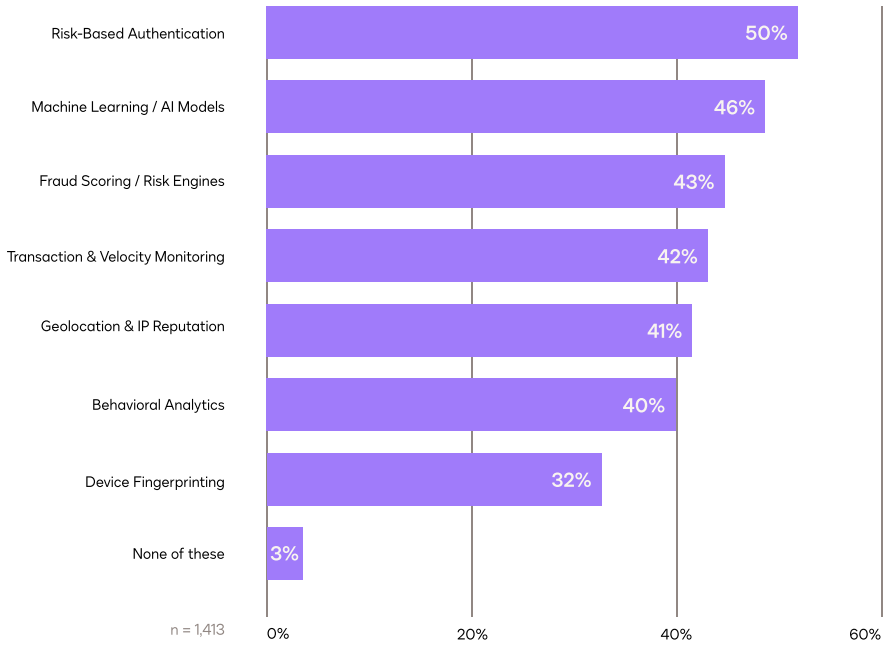


When determining what level of authentication to require of a user in a particular interaction, what is this decision based on?

In addition to following a variety of methods to assess customer risk, organizations use a range of tools. The most popular are risk-based authentication tools, which automatically adjust the required level of identity verification for each interaction based on a customer's assessed risk. A high-risk customer, for example, might trigger a biometric check, while a low-risk customer may only have to complete MFA.

Risk-based authentication is most popular tool for assessing customer risk

Tools for Assessing Authentication Risk



Which of the following does your organization use when assessing the risk associated with a particular interaction?

74%

of organizations plan to invest more in IDV solutions in the future.

Organizations plan to continually invest in IDV

As the identity fraud landscape evolves and organizations continue to monitor strategies and tools for assessing risk and preventing fraud, no matter the size, region, or industry, they remain steadfast on one belief: Technology is the key to addressing this growing problem.

Decision-makers are particularly interested in the role biometrics and generative AI will play in combating fraud. Compared to their current methods of authenticating and verifying users:

84%

of respondents believe biometric authentication will be more effective at reducing the risk of customer fraud.

82%

of respondents believe generative AI will be more effective at reducing the risk of customer fraud.

78%

of respondents believe risk-based assessment will be more effective at reducing the risk of customer fraud.

Among these three solutions, generative AI is considered the most appealing for customers, but many respondents are still wary of pushback. While 46% of organizations agree that their customers will be frustrated or upset if they adopt generative AI as part of their IDV process, 59% believe they will see a significant uptick in fraud unless they do adopt it.

Conclusion

Organizations around the world face a new risk landscape. The rise of generative AI and widespread adoption of digital transactions, coupled with lack of customer awareness on best security practices, have created a perfect storm for identity fraud. As the threat of fraud grows, the world's leading businesses are investing in cutting-edge tools like identity verification for protection.

Our survey led to one finding above all else: Technology is the key to catching identity fraud throughout the customer journey while also reducing unnecessary spend.

With IDV, businesses can build powerful defenses to safeguard their reputations and bottom lines. Even in tight business environments, investing in IDV brings long-term benefits of risk reduction and strong ROI. Customers, in turn, gain peace of mind knowing their personal information is secure—while still enjoying a seamless digital experience.

The costs of identity fraud will only rise as AI advances. For organizations seeking to protect their customers, defend their reputations, and appeal to young generations more accustomed to engaging with digital identity verification tools, taking a proactive stance and investing in anti-fraud technology has never been more important.

Key recommendations

Re-evaluate your anti-fraud defenses.

There's a reason 74% of organizations evaluate new solutions at least once a year: Fraudsters are constantly learning and adopting new techniques. Businesses need to update their defenses accordingly. The easiest way to do so is to continuously seek out and work with vendors who regularly refine their own tools in defense against the latest tactics and challenges.

Invest in AI-powered technology.

According to the majority of decision-makers surveyed, the best way to mitigate the financial risk of identity fraud is investing heavily in technology. Rather than spending valuable resources on reactive measures, such as insurance or more time hiring more talent, investing in AI-powered IDV solutions gives businesses the best advantage in fighting identity fraud, especially sophisticated threats like generative AI.

Identify the most vulnerable stages of your customer lifecycle.

Account creation, login, and payment authorization are the steps of the customer journey most impacted by identity fraud, according to our survey. These can be worthwhile areas to focus your initial efforts, but we recommend working with a qualified team to map out your own customers' journey and identify where your business faces the most risk.

Move past the false "fraud protection vs. user experience" dichotomy.

The most savvy respondents in our survey noted that better fraud measures do not require compromising on user experience. On the contrary, IDV can complement the customer experience and enhance brand reputation. To provide the best IDV experience and ensure smooth implementation, encourage collaboration among your risk, product, and growth teams and prioritize user-friendly products equipped with automation.

Calculate the ROI of your anti-fraud investments.

Organizations that invested significantly more than their peers in IDV tended to save more than those that invested the same. To set yourself up for similar ROI, assess a few factors when researching new technology, including your expected decrease in fraud cost, headcount savings through automation, lower customer acquisition costs, and revenue gains from new customers.

Embrace the expectations of young consumers.

Millennial and Gen Z decision-makers at organizations are more likely to see the value of IDV tools in improving brand perception and security. There's a similar parallel with their customers: Millennial and Gen Z consumers prefer innovative technologies like biometric authentication to other methods. Businesses can rest assured that adopting advanced technology will earn them the respect of young customers and employees—setting their organizations up for success now and into the future.

Learn more about Docusign Identify and Entrust.

Appendix: Methodology

The Future of Global Identity Verification report is based on data collected during a quantitative, global online survey that ran from November 6, 2024 to December 4, 2024. During the data collection process, our research team[2] engaged with business and IT decision-makers across industries and regions. The decision-makers surveyed in this report work at organizations with anywhere from 150 to 10,000+ employees and share the challenge of verifying their customers' identities.

Total N=1,413

Audience	
Current IDV Users	N=976
User Auth / Digital Users but no IDV	N=309
Manual Auth / No IDV Users	N=128
Market*	
United States & Canada NAM	N=304
United Kingdom EMEA	N=227
Germany EMEA	N=233
France EMEA	N=226
Mexico LATAM	N=104
Brazil LATAM	N=104
Australia APAC	N=102
Japan APAC	N=113

*Each market was fielded in their primary language

Org Size	
150-499	N=254
500-999	N=266
1,000-2,499	N=274
2,500-4,999	N=204
5,000-9,999	N=213
10,000+	N=202

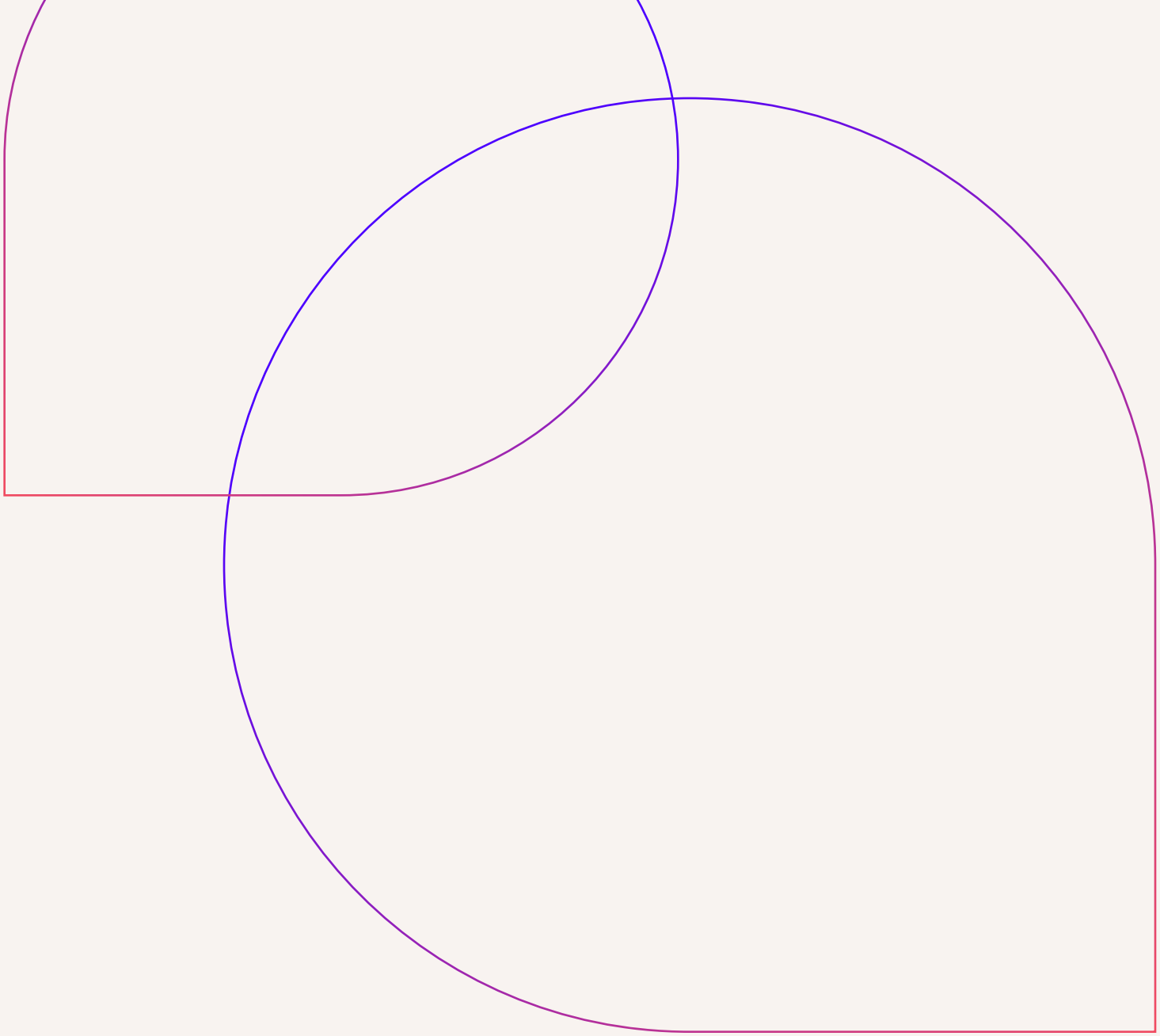
Industries surveyed

- Banking
- Professional services
- Education
- Financial services
- Healthcare
- Insurance
- IT services
- Life sciences
- Pharmaceuticals
- Retail & eCommerce
- Construction & engineering
- Manufacturing
- Real estate
- Telecommunications
- Energy & utilities

Roles surveyed

- IT operations / IT department
- IT security
- Purchasing and supply chain management
- Operations
- Customer experience
- Product management
- Risk management / compliance
- Fraud analysis
- Human resources
- Customer service
- Legal
- Sales

2 Docusign and Entrust commissioned TL;DR Insights, a market research company, to conduct the survey.



About Docusign and Entrust

Docusign brings agreements to life. Over 1.6 million customers and more than a billion people in over 180 countries use Docusign solutions to accelerate the process of doing business and simplify people's lives. With intelligent agreement management, Docusign unleashes business- critical data that is trapped inside of documents. Until now, these were disconnected from business systems of record, costing businesses time, money, and opportunity. Using the Docusign Intelligent Agreement Management platform, companies can create, commit to, and manage agreements with solutions created by the #1 company in e-signature and contract lifecycle management (CLM).

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

Docusign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105
docusign.com

For more information
sales@docusign.com
+1-877-720-2040