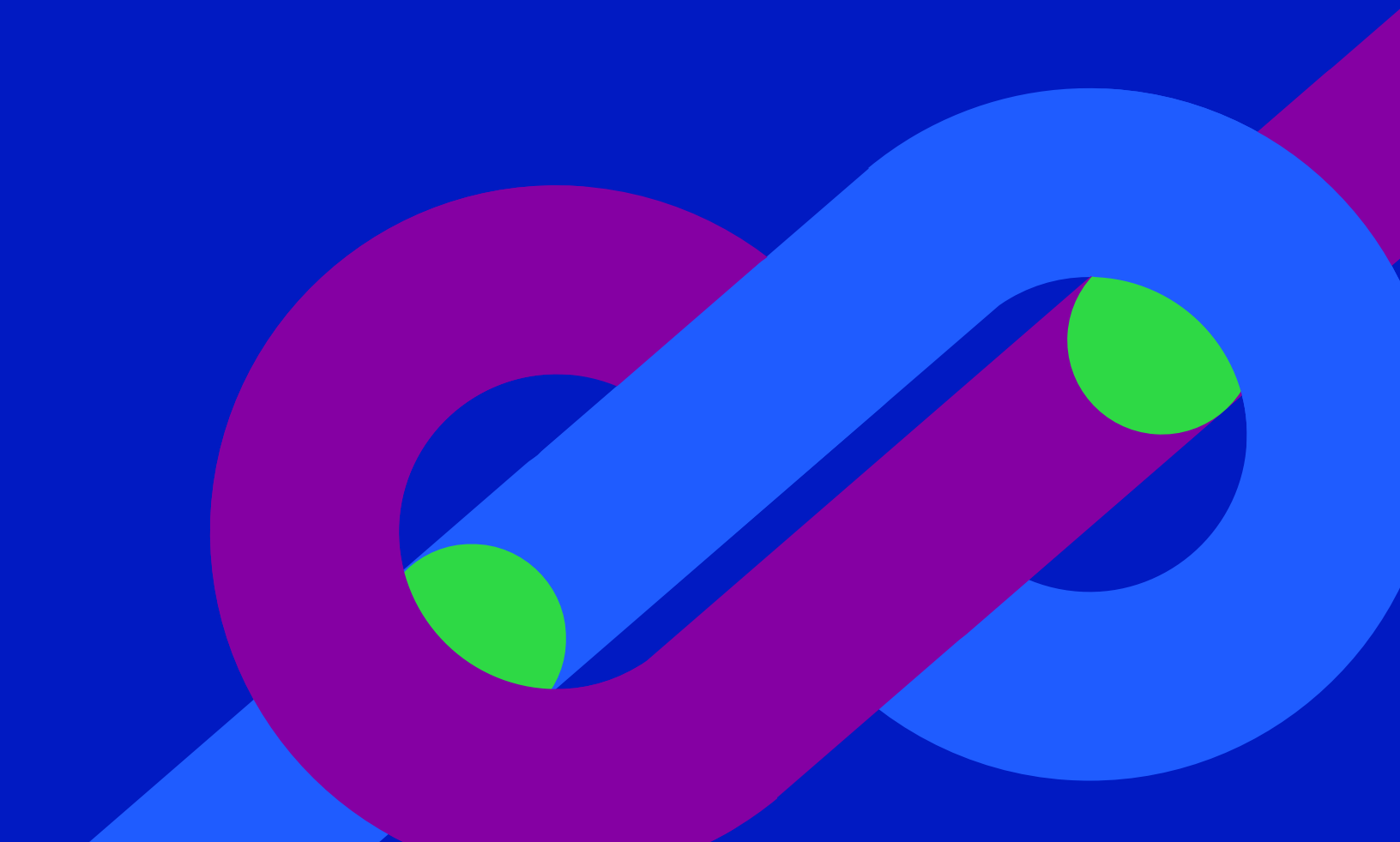
telesign

REPORT

2023 Telesign Trust Index

Trust matters

The critical role of trust
in the digital economy



Trust matters in all facets of life, society, and business.

The 2023 Telesign Trust Index reveals just how much trust matters in our digital world.

KEY FINDINGS

It is said that trust takes years to build, seconds to break, and forever to repair.

The 2023 Telesign Trust Index proves how true this statement is in the digital world. Data from the report supports the following insights:

- Consumers overwhelmingly agree that it is the responsibility of companies – and not individuals – to protect their digital privacy.
- Consumers fear digital fraud and believe it is on the rise.
- Consumers will hold companies accountable if they become victims of fraud.
- Digital fraud affects the financial and psychological health of consumers.
- Even a single breach or data leak can cause significant harm to a company's reputation and bottom line.

KEY FINDINGS

Fraud victims risk more than money

Digital fraud affects the financial and psychological health of consumers.

30%

of consumers surveyed reported they were victims of fraud in the past **three years**

61%

of victims report financial losses, and one-third of victims report losses of **more than $1,000**

40%

cite mental health concerns and **44%** characterize the incident as having a negative impact on them

KEY FINDINGS

Data breaches have a profound, negative impact on brand perception

Even a single breach or data leak can cause significant harm to a company's reputation and bottom line.

43%

of data breach victims personally **stopped associating** with the brand altogether

44%

of data breach victims are reported to have told friends and family **not to associate** with the brand

30%

of data breach victims shared the incident on social media, **amplifying negative** brand perceptions

Consumers fear digital fraud and believe it is on the rise

Consumers overwhelmingly agree that it is the responsibility of companies – and not individuals – to protect their digital privacy and will hold companies accountable if they become victims of fraud.

23%

of consumers shared that they would rather never eat chocolate again or be audited by the IRS **than become a victim** of digital fraud

50%

of consumers polled indicated their apprehension regarding telephone and digital fraud has **increased** in the last two years

94%

of consumers surveyed agree that businesses **bear responsibility** for protecting their digital privacy

KEY FINDINGS

Digital fraud targets a new demographic

While elderly fraud has captured the media's attention, digital fraud targets a different demographic. Forget the stereotypical image of a grandmother being scammed by a robocall.

46%

of digital fraud victims fall between the ages of 25-44, indicating that **Millennials are more than 4x** as likely to be victimized than their parents or grandparents (aged 65+)

20%

of Millennial victims of digital fraud **experienced account hacking**, while **14% experienced phishing scams**

66%

of fraud victims surveyed **were women**, compared to **34% men**

Digital services increase likelihood of being a fraud victim

Greater exposure on the internet leads to a statistically higher probability of becoming a victim of fraud.

Ages 18-34

spend the most time online, followed by ages 35-52 (all spending 3+ hours per day online)

56%

of recent fraud victims reported using **6 or more digital services**

2x

Having a child in the household **nearly doubles the likelihood of being a fraud victim**

KEY FINDINGS

Consumers increasingly fear online fraud, yet fail to take action

Increases in digital adoption and fraudulent activity underscore the importance of effective fraud management to meet today's customer experience expectations. But there's a gap in level of concern from consumers and their own willingness to act.

45%

of consumers do not actively protect themselves against cybercrime, emphasizing the **urgent need for businesses to prioritize comprehensive fraud management**

20%

of consumers said they **won't invest in annual data protection services**

Businesses need to take action to protect their customers

The COVID-19 pandemic accelerated digital adoption, creating more opportunity for fraudsters to take advantage of customers who are not actively protecting their digital identities.

43%

of consumers indicated that they are either **extremely or somewhat concerned that digital fraud is on the rise**

50%

of all consumers said their **fear of becoming a victim has increased** over the last two years

#1

greatest "trust-breaking" event for an organization and its customers, per IDC's recent findings, is the **unauthorized release of personally identifiable information through a data breach**

IDC Survey Spotlight, "How Do We Break Trust", doc #US51357423, November 2023

Key insights for businesses

Digital technologies are transforming our world, and often faster than business has been able to transform its digital infrastructure. The pandemic accelerated this transformation years ahead of what most experts thought was possible.

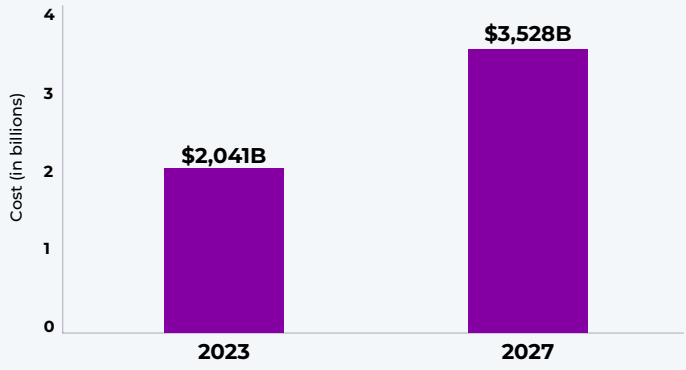
Looking at the growth at a micro level, Statista reports the total transaction value in the digital payments segment, alone, is projected to reach $2,041B in 2023 and $3,528B by 2027. On the macro level, The World Economic Forum estimates 70% of new value created in the economy over the next decade will be based on digitally enabled platform business models.

With all the promised benefits of a digital economy comes real obstacles. As the volume of digital business rises so does the potential for cybercrime, including digital fraud.

DIGITAL PAYMENTS

Total transaction value

Statista



70%

of **new value** created in the economy over the next decade will be based on digitally enabled platform business models.

Economic Forum

The value of reassuring consumers in a digital world

The 2023 Telesign Trust Index is a first-of-its-kind study to examine the critical role that trust plays in the digital world. The findings underscore the impact of fraud on consumers and the obligation of companies to ensure digital privacy protections and continuous trust in all digital transactions. The study showed that consumers fear fraud is on the rise. It also highlighted the huge toll it takes on them, personally and in turn, on the companies that serve them.

It's sometimes said that people fear what they don't understand. There is an opportunity for brands to adopt new technologies that ensure their digital infrastructure is built on a foundation of trust and to differentiate themselves by the lengths they will go to protect their end users data.

Consumers value their security and their time in their digital transactions. They are often making split second decisions about which brands they can trust with their data. They seek validation that the companies they engage with are trustworthy. As this study highlights, customers have high expectations that companies they do business with will protect them.

The study showed that consumers fear fraud is on the rise... and it proved the huge toll it takes them, personally, and in turn, on the companies that serve them.

What does it take to protect and defend the world's leading brands and their end-users from fraud and loss?

Establishing and maintaining trust in business transactions has become mission critical for organizations. However, not all digital fraud protection and safety strategies and technologies employed by companies today are created equal.

Advancements in technology, including the use of powerful ML (machine learning), will enable companies to create an environment of Continuous Trust. The future of preventing fraud, protecting user privacy data, and maintaining the continuous trust of their customers is not passive.

By implementing proactive fraud prevention strategies and digital privacy protections and technologies, the promise of the digital economy is realized. The businesses who win in the digital economy will be those that are the most trusted.

What are the latest digital fraud trends businesses should be aware of?

Fraudulent tactics evolve quickly, making it essential for companies to stay up to date on the most prevalent schemes and prevention strategies in order to build and keep customer trust. The latest tactics fraudsters use to steal from businesses and their customers include:

Fake accounts

Fraudsters create fake accounts to manipulate digital likes or installation numbers to benefit themselves. Fake accounts are created using stolen email addresses, phone numbers, and usernames to build deceptive profiles designed to trick security checks.

Once onboarded, fake users spread misinformation, network with unsuspecting valid users, impersonate brands, and commit fraud. Fake users ruin company ecosystems, forcing businesses to restrict transactions from platforms without fake user protections in place.

Onboarding issues (i.e. long sign-up process)

A customer's initial excitement after downloading an app is easily deflated if the sign-up process contains too much friction. Consumers today expect some level of onboarding friction; however, too much can drive them away.

Appropriate friction is necessary when interacting with digital services such as online banking to detect and block fraudsters from creating accounts. Appropriate friction keeps customers safe and secure while onboarding, enhancing the customer experience.

Account takeover

Account takeover (ATO) attacks are when hackers gain access to personally identifiable information (PII), which they can leverage to take over the accounts attached to this information.

ATO is bolstered by increases in data breaches, social engineering attacks, phishing, and brute force attacks. Fraudsters can use the stolen PII and accounts to take over apps and make fraudulent purchases. They also create clone apps, designed specifically to steal PII and other credentials from victims who download them.

Promo abuse

Promo abuse is one of the most expensive types of fraud, with **78%** of retailers reporting a serious increase in recent years.

Promo abuse occurs when users create multiple accounts to access and exploit free trials, coupons, referral bonuses, and more. These accounts, which are often used once then abandoned, cause serious issues for businesses. Promo abuse costs companies via customer acquisition costs and revenue.

Methodology

This Telesign Trust Index Survey was fielded online and reached a total of n=1,000 respondents. Respondents were U.S. adults aged 18+; a subset of which have been victims of digital fraud within the past three years. The survey was fielded in January 2023. The margin of error for a sample size of 1,000 is +/- 3.10 percentage points at a 95% confidence level.

About Telesign

Telesign provides Continuous Trust™ to leading global enterprises by connecting, protecting, and defending their digital identities. Telesign verifies over five billion unique phone numbers a month, representing half of the world's mobile users, and provides critical insight into the remaining billions. The company's powerful machine learning and extensive data science deliver identity with a unique combination of speed, accuracy, and global reach. Telesign solutions prevent fraud, secure communications, and enable the digital economy by allowing companies and customers to engage with confidence. Learn more at www.telesign.com and follow us on Twitter at @Telesign.

telesign