2023 State of Fraud

WHITE PAPER

telesign

Despite the best efforts of businesses and technology vendors, fraudsters continue stealing billions of dollars every year. In 2022, U.S. fraud victims lost nearly $8.8 billion to fraud[1], and global losses are expected to reach $48 billion USD in 2023[2] and may reach $95.9 billion USD by 2027.[3]

In addition to significant financial losses, fraud damages customer loyalty, brand reputation, and brand trust, all of which are difficult to repair. Many victims of fraud report that they no longer associate with the brand where their data was compromised and they frequently urge their friends, family, and digital followers to stop as well.

To reduce fraud and increase customer satisfaction, businesses must seek effective fraud prevention solutions that protect consumers without adding friction to their digital experience. This white paper discusses recent trends in online fraud, presents new data about the personal and business impact of fraud, and explores modern fraud prevention strategies and solutions.

In 2022, U.S. fraud victims lost nearly

$8.8B

Fraud damages customer loyalty, brand reputation and brand trust, all of which are difficult to repair.

The evolving fraud landscape

Fraudsters and other cybercriminals are often among the earliest adopters of new trends and technologies, harnessing their innovation to power increasingly sophisticated threats.

Growing corporate data breaches

In the past three years, 27% of global companies and 34% of North American companies suffered a data breach that cost them between $1M and $20M USD, and only 14% of global companies reported that they experienced no data breaches.[4] While most breaches are in the healthcare, financial services, and manufacturing industries[5], the impact of compromised data reaches much further. After a breach, stolen account credentials and Personally Identifiable Information ("PII") may be published and/or sold worldwide, providing fraudsters the information they need to take over existing accounts and create new ones. In 2022, more than 422 million people were affected by data breaches, leakage, or exposure.[6]

Generative AI-based threats

ChatGPT and other generative AI make it easier for fraudsters to create convincing written, audio, and video "deepfake" phishing lures that bait victims into compromising their own devices and accounts, and may help synthetic identities and bot-created accounts better masquerade as legitimate users. Generative AI could also make it easier for fraudsters to obtain PII from unsuspecting victims. For example, cybersecurity researchers have used ChatGPT to generate a new keylogger that automatically adapts to a victim's environment to evade detection while collecting account and credit card information.[7]

Exploitation of new payment methods

As the number of different payment options grows, fraudsters are keeping pace with new ways to exploit the systems. For example, the buy now, pay later (BNPL) market is estimated to reach $309.2 billion USD in 2023, with an expected annual growth rate of 25.5%.[8] However, BNPL fraud is growing even faster, with a 211% year-over-year increase for an estimated loss of $48 billion USD in 2023.[9]

Common fraud tactics

Fraud technologies and strategies are constantly evolving. Some of the most common types of fraud are discussed below.

New account fraud/ synthetic identity fraud

In new account fraud, a fraudster creates an account using a real person's credentials and identity. In synthetic identity fraud, a fraudster uses PII from one or more real people to create and support a new fake online persona. In 2022, 46% of organizations faced synthetic identity fraud[10], and the numbers are expected to climb. Additionally, 60% of businesses reported bots and fake users during onboarding.[11]

Account takeover (ATO)

ATO occurs when fraudsters obtain login credentials for a legitimate existing account, allowing them to bypass security measures that prevent the creation of new fraudulent accounts. ATO is increasingly common—according to the nonprofit Identity Theft Resource Center, 61% of reported misuse of identity cases last year were a result of ATO.[12] Some experts estimate that 22% of U.S. adults have been ATO victims, with an average loss of $12,000.[13]

Promotion and discount abuse

Promotions and discounts — including signup and referral bonuses, discounts on purchases, loyalty rewards, and more — can be an effective way to encourage more signups and purchases. The right promotional offer can entice visitors to return to an abandoned online shopping cart or visit a physical store to redeem it.

Unfortunately, promotions and discounts can be easy to abuse. Misuse ranges from individuals creating second accounts to access discounts to automated attacks that create multiple accounts that appear eligible for the promotion. Promotion abuse is widespread, and 73% of retailers report that they experienced promotion abuse in the previous twelve months.[14]

22%

of U.S. adults have been ATO victims, with an average loss of $12,000.

Fraud's personal and business impact

This section contains results from original research in the 2023 Telesign Trust Index. (Learn about our methodology here.)

Fraud harms consumers' financial and mental health

The 2023 Telesign Trust Index shows that consumers are increasingly cautious about fraud, and with good reason: many fraud victims report damage to both their financial and psychological health. Results include the following:

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

Brands suffer when consumers become fraud victims

Overall, 94% of consumers believe that businesses bear responsibility for protecting their digital privacy. Brands that fail to deliver protection may suffer in the marketplace:

43%

of data breach victims **stopped associating** with the brand.

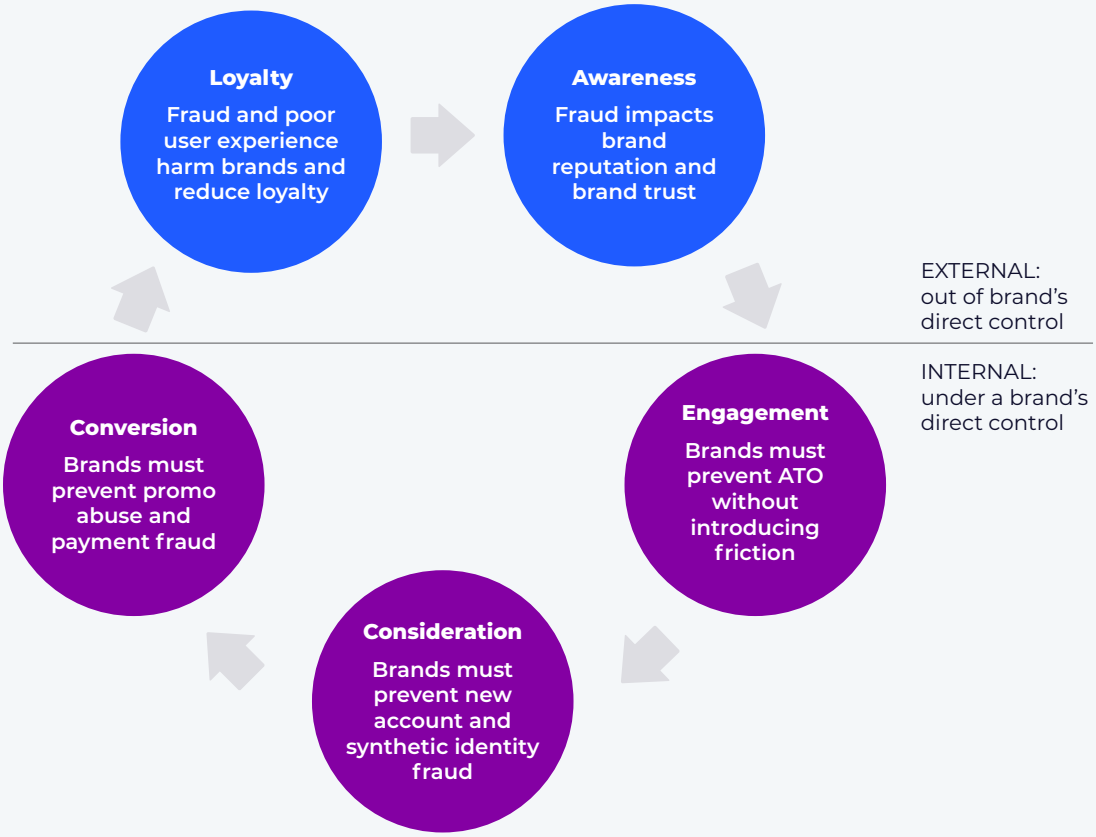
44%

of data breach victims advised friends and family **to stop associating** with the brand.

30%

of data breach victims **amplified their negative perceptions** by sharing the incident on social media.

Figure 1: Fraud prevention impacts every stage of the consumer journey.



The message is clear:

In addition to direct financial losses, fraud causes long-term damage to customer loyalty, brand reputation, and brand trust. Figure 1 illustrates how fraud prevention can influence all stages of the consumer journey, even those that aren't under a brand's direct control.

Finding the balance between security and ease of use

Best practices in fraud prevention rely on a broad spectrum of technologies and techniques, including multi-factor authentication (MFA), digital identity verification, and analysis of thousands of potential fraud indicators based on up-to-the-minute intelligence.

Unfortunately, effective fraud prevention isn't the only consideration. According to a recent study, 24% of shoppers will abandon their shopping carts if they are required to create an account, 18% will abandon their carts if they don't trust the site with their payment information, and 17% will leave if the checkout process is too long or complicated.[15] Clearly, consumers expect brands to protect their digital privacy and simultaneously deliver a seamless digital experience.

Advances in fraud prevention — including deployment of machine learning that can analyze vast amounts of data in milliseconds — make it faster and easier to flag and block potential fraud without compromising user experience. Ideal solutions will include:

Simple and secure onboarding that stops new account and synthetic identity fraud without a slow and complicated account creation process

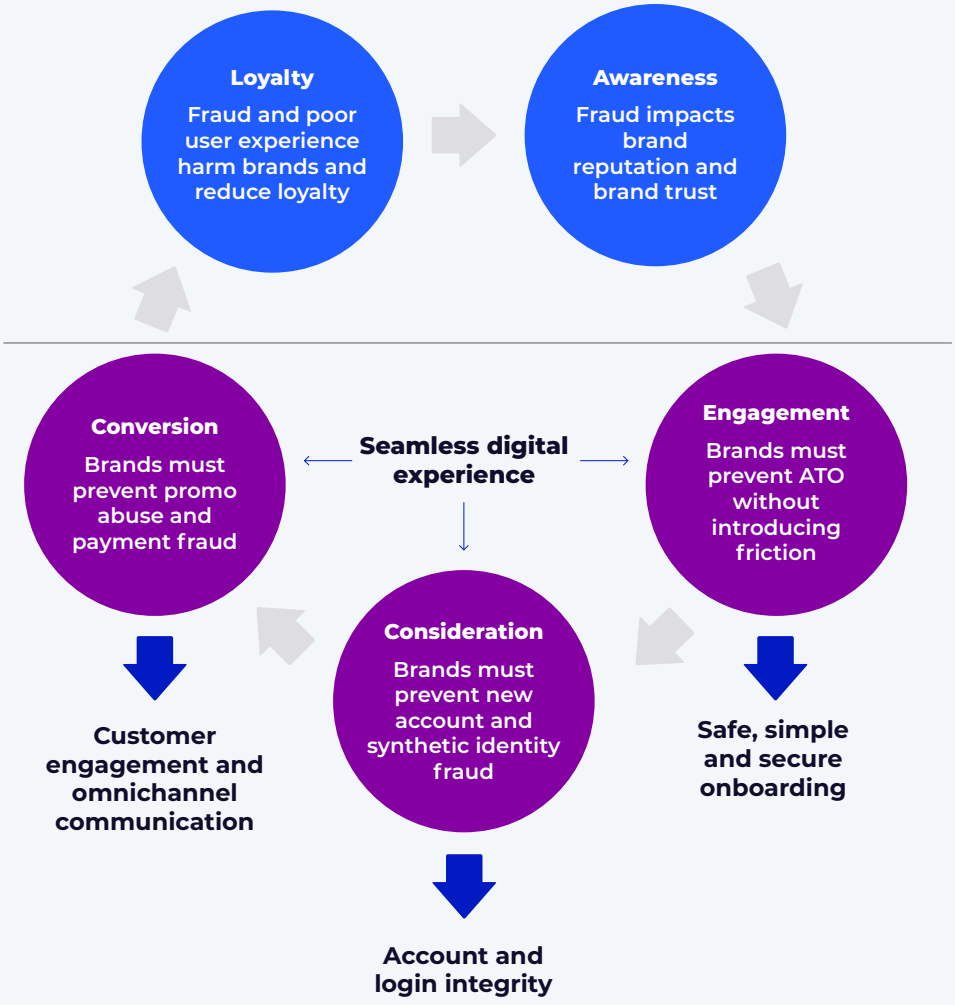
Account and login integrity features that block ATOs and protect consumer accounts

Features that end coupon abuse, free trial loopholes, and referral fraud while allowing eligible consumers to enjoy the discounts and rewards that they've earned

Secure omnichannel communications to send the right information and offers at the right time to encourage and reward legitimate eligible consumers

Figure 2 shows how fraud prevention solutions can protect both brands and consumers and contribute to seamless experiences throughout the consumer journey.

Figure 2: Brands will benefit from fraud prevention solutions that help eliminate friction as well as fraud.



Telesign solutions improve security and enhance consumer experience

The Telesign Trust Engine and Omnichannel Experience solutions deliver industry-leading features that boost security and minimize friction throughout every step of the customer journey.

Onboarding

Secure onboarding that keeps fake accounts out of your digital experience is your first defense against fraudster damage. Telesign makes it easy to welcome new accounts quickly and block fraudsters with features that help you:

- Incorporate real-time digital identity and behavioral risk signals into sign-up flows
- Analyze thousands of digital attributes across phone, email, and IP datasets to allow, flag, or block new signups in milliseconds
- Strengthen KYC checks without slowing or complicating signups
- Prevent promotion fraud by blocking accounts created to abuse discounts, free-trial loopholes, and referrals

Account and login integrity

Failing to protect consumers from ATO costs more than money: it can irrevocably harm brand reputation and trust. Telesign helps protect consumer accounts with features that:

- Evaluate multiple ATO risk signals to confirm a consumer's identity at every login
- Streamline MFA to deliver robust verification with minimal friction
- Deliver secure one-time passcodes (OTP) on platforms that consumers prefer

Secure omnichannel communications

Telesign's powerful communication solutions empower organizations to communicate with customers throughout their journey for a low-friction experience and meaningful engagement that includes:

- Real-time secure notifications and messages on platforms including WhatsApp and Viber and protocols including RCS, SMS, and MMS
- Delivering innovative content that includes branding, pictures, GIFs, video, and chatbots
- Personalized offers and customer care communications

Telesign and Continuous Trust™

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. Our 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 https://www.telesign.com.

Methodology for the Telesign Trust Index Survey

The survey was fielded online in January 2023 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 margin of error for a sample size of 1,000 is +/- 3.10 percentage points at a 95% confidence level.

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

Telesign.com

1 https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

2 https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/

3 https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report

4 https://www.pwc.com/dti2023

5 https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

6 https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

7 https://www.darkreading.com/endpoint/ai-blackmamba-keylogging-edr-security

8 https://www.globaldata.com/store/report/buy-now-pay-later-market-analysis

9 https://bankautomationnews.com/allposts/risk-security/by-the-numbers-bnpl-fraud-attempts-jump-211-yoy/

10 https://www.securitymagazine.com/articles/99268-46-percent-of-organizations-faced-synthetic-identity-fraud-in-2022

11 https://www.telesign.com/report/modern-approaches-to-digital-onboarding

12 https://www.idtheftcenter.org/wp-content/uploads/2023/05/ITRC_2022-Trends-in-Identity-Report_Final.pdf

13 https://www.security.org/digital-safety/account-takeover-annual-report/

14 https://www.pymnts.com/study/beyond-ecommerce-fraud-policy-abuse-retail-fraud-prevention/

15 https://baymard.com/lists/cart-abandonment-rate

telesign