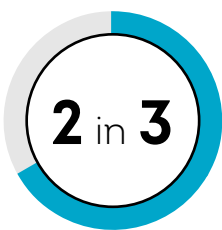TransUnion

# GLOBAL DIGITAL
# FRAUD TRENDS

### Rising customer expectations amid evolving fraud threats

# Summary

The COVID-19 pandemic demonstrated how cybercriminals follow the money, and showcased their skill and ingenuity in targeting vulnerable consumers and businesses. They adapted to economic shifts and wreaked havoc. Coinciding with this, accelerated consumer adoption of and preference for digital channels elevated expectations around both experience and security. Businesses need to optimize efforts to counter potential fraud risks whilst aspiring to offer the smoothest customer experiences possible. The fact two in three consumers surveyed globally by TransUnion in January 2022 said they're likely to switch companies for a better digital experience underscores the strategic need to get this right.[1]

**2 in 3** consumers globally surveyed by TransUnion in Jan. 2022 said they're likely to switch companies for a better digital experience

Businesses should view fraud and identity solutions as not only defensive measures but assets that can support customer acquisition and retention. The right approach offers a better understanding of consumers, helps to improve the onboarding experience, and provides the foundation to build trust between business and consumer.

| Global growth in the suspected digital fraud rate [2] | Travel and leisure industry: Largest growth in suspected digital fraud worldwide [2] | Financial services digital fraud growing rapidly [2] | Shipping fraud: Top type of digital fraud worldwide [2] |
|---|---|---|---|
| **2019–2021** | **2019–2021** | **2019–2021** | **2019–2021** |
| +52.2% | ↑110.7% | ↑60.5% | ↑1541.8% |
| **2020–2021** | **2020–2021** | **2020–2021** | **2020–2021** |
| +9.4% | ↑68.4% | ↑33.5% | ↑780.5% |

TransUnion

# Contents

TransUnion

# Introducing TransUnion's 2022 Global Digital Fraud Trends Report

Our annual report presents a comprehensive, global view of the dominant fraud threats that have affected both businesses and consumers in 2021. We overlay this with consumer research (conducted at the start of 2022) to understand how digital adoption has influenced consumer preferences and attitudes toward fraud and shaped expectations. Finally, we conclude by identifying a number of opportunities these findings hold for businesses.

## Fraud increases as economic activity evolves

As economies shift and consumer buying behavior changes, fraudsters seek out potential weaknesses. Between 2019–2021, the rate of suspected digital fraud grew 52.2%. Travel and leisure and financial services organizations suffered an increased suspected online fraud rate as tourism resumed and online banking became the norm.[2]

## Digital experience expectations accelerate

Consumers expect digital experiences to be secure, fast and convenient. Failure to meet these standards and they'll likely abandon. Two-thirds of consumers told us they'd switch companies for a better digital experience, with Gen Z and Millennials universally more likely to switch than older generations (67% and 70%, respectively compared to 56% for Gen X and 45% for Baby Boomers).[1]

## Building trust in digital channels is essential to the customer relationship

Consumers want businesses to take the lead by creating secure experiences they trust, be it through strong authentication processes or education on fraud threats. Businesses need to help consumers better protect themselves. Just one in three targets of digital fraud surveyed worldwide said they placed a fraud alert on their credit report (32%) or froze their credit (36%).[1]

TransUnion

# Fraudsters shadow consumer preferences and growth sectors

## Global consumer trends

### 1 in 3
consumers gobally now conduct anywhere between 51%–75% of their transactions online [1]

### 15%
conduct anywhere between three-quarters to 100% of their transactions online [1]

### 48%
of both Millenials and Gen Xers stated they conduct the majority of their transactions online [1]

**Figure 1: Consumer preferences for digital transactions by region** [1]

Q48: What percentage of your transactions (finances, retail, business, etc.) are done online?

| Region | 1% - 25% transactions | 26% - 50% transactions | 51% - 75% transactions | 76% - 100% transactions |
|---|---|---|---|---|
| BRAZIL | 20% | 23% | 32% | 25% |
| CANADA | 27% | 30% | 27% | 16% |
| CHILE | 11% | 21% | 36% | 32% |
| COLOMBIA | 29% | 27% | 31% | 14% |
| DOMINICAN REPUBLIC | 36% | 27% | 21% | 15% |
| HONG KONG | 28% | 39% | 24% | 9% |
| INDIA | 5% | 46% | 41% | 9% |
| KENYA | 27% | 30% | 30% | 13% |
| MEXICO | 16% | 27% | 40% | 17% |
| PHILIPPINES | 31% | 35% | 25% | 9% |
| PUERTO RICO | 27% | 26% | 24% | 23% |
| SOUTH AFRICA | 26% | 35% | 27% | 12% |
| SPAIN | 22% | 28% | 31% | 20% |
| UNITED KINGDOM | 18% | 32% | 34% | 16% |
| UNITED STATES | 26% | 33% | 30% | 12% |

TransUnion

However, these global responses hide regional and demographic differences.

**81%** of Baby Boomers in Chile stated they perform over 50% of transactions online versus 53% of Gen Z.[1]

**38%** of Baby Boomers in India, on the other hand, indicated they do most of their transactions online compared to 62% of Gen Z.[1]

## Fraudsters follow consumer behavior

Fraudsters have shadowed consumer preferences for online transactions and targeted those industries that experienced spikes in usage. TransUnion's global intelligence network analyzed billions of digital transactions and identified how bad actors took advantage of the economic disruption.

## Findings showed:

A **52.2%** increase in the rate of suspected digital fraud globally between 2019 and 2021, with a 9.4% uplift in the rate during the 2020 to 2021 period.[2]

Between 2020 and 2021, the percentage of suspected digital fraud attempts against the travel and leisure industry increased **68.4%** around the globe.[2]

Shipping fraud, business identity theft and identity mining/phishing were increasingly prevalent threats – rising 780.5%, 113.8% and 104.8%, respectively from 2020 to 2021.[2]

## Fraud risk by industry

**Figure 2: Suspected digital fraud rate percentage change by industry** [2]

Transaction periods Jan. 1 - Dec. 31, 2019, 2020 and 2021

| | | |
|---|---|---|
| **Travel and leisure** | **Gaming** | **Financial services** |
| 2019–2021 | 2019–2021 | 2019–2021 |
| **+110.7%** | **+68.6%** | **+60.5%** |
| 2020–2021 | 2020–2021 | 2020–2021 |
| **+68.4%** | **+32.6%** | **+33.5%** |
| **Insurance** | **Ecommerce** | **Telecommunications** |
| 2019–2021 | 2019–2021 | 2019–2021 |
| **+54.3%** | **+53.9%** | **+45.6%** |
| 2020–2021 | 2020–2021 | 2020–2021 |
| **-2.2%** | **-11.3%** | **-4.0%** |
| **Gambling** | **Logistics** | **Communities** (online dating, forums, etc.) |
| 2019–2021 | 2019–2021 | 2019–2021 |
| **+29.4%** | **-16.7%** | **-23.5%** |
| 2020–2021 | 2020–2021 | 2020–2021 |
| **+19.2%** | **-35.9%** | **+9.8%** |

Travel and leisure was consistently in the top three industries across regions analyzed suffering an increase in the rate of suspected online fraud from 2020 to 2021, primarily via credit card fraud.

Financial services also remained a prime target. Our data indicates financial services providers suffered increases in the rate of suspected digital fraud attempts from 2020 to 2021 originating from all but one region analyzed, with fraudsters utilizing true identity theft as their method of choice. This is an area of increasing concern with reported true identity theft fraud growing 26.4% over the past year, and 81.8% over the past two years across industries.[2]

True identity theft increased

**81.8%**

across industries between 2019 and 2021

## Growth in fraud types

**Figure 3: Top 10 fastest growing fraud types globally** [2]

When comparing 2019 to 2021 and 2020 to 2021

| 2019–2021 | | 2020–2021 | |
|---|---|---|---|
| 1 | Shipping fraud **1541.8%** | 1 | Shipping fraud **780.5%** |
| 2 | ACH/Debit fraud **531.3%** | 2 | Business identity theft **113.8%** |
| 3 | Business identity theft **165.7%** | 3 | Identity mining/Phishing **104.8%** |
| 4 | First party fraud **91.1%** | 4 | First party fraud **55.8%** |
| 5 | True identity theft **81.8%** | 5 | Scammer/Solicitation **53.9%** |
| 6 | Scammer/Solicitation **57.3%** | 6 | True identity theft **26.4%** |
| 7 | Friendly fraud **54.1%** | 7 | Application fraud **19.3%** |
| 8 | Synthetic identity theft **41.1%** | 8 | Account takeover/Hijacking **6.4%** |
| 9 | Application fraud **38.4%** | 9 | Friendly fraud **5.5%** |
| 10 | Profile misrepresentation **6.5%** | 10 | Synthetic identity theft **5.5%** |

The growth in suspected instances of shipping fraud between 2019 and 2021 again illustrates how fraud follows changes in consumer behaviour. In this case, lockdowns and remote working increased online transactions for consumer goods which fueled demand for shipping and delivery services. These activities presented opportunities for criminals to commit different types of shipping fraud.

Suspected instances of identity theft and phishing also grew. These threats correspond with consumer fears which revolve around identity theft, phishing scams, account takeover and credit card theft.

# 62%

of consumers reported being concerned about falling victim to identity theft [1]

TransUnion

## Top consumer digital fraud concerns

**Figure 4: Top three fraud concerns for consumers by country** [1]

(Consumer could select all that apply)



### Brazil
Credit card fraud: **76%**
Identity theft: **68%**
Account takeover: **40%**

### Canada
Credit card fraud: **63%**
Identity theft: **59%**
Phishing: **44%**

### Chile
Credit card fraud: **70%**
Identity theft: **65%**
Account takeover: **57%**

### Colombia
Identity theft: **75%**
Credit card fraud: **73%**
Account takeover: **58%**

### Dominican Republic
Credit card fraud: **78%**
Identity theft: **72%**
Account takeover: **56%**

### Hong Kong
Credit card fraud: **61%**
Identity theft: **59%**
Phishing: **46%**

### India
Credit card fraud: **41%**
Account takeover: **37%**
Vishing: **35%**

### Kenya
Credit card fraud: **68%**
Identity theft: **61%**
Phishing: **60%**

### Mexico
Credit card fraud: **73%**
Identity theft: **70%**
Account takeover: **49%**

### Philippines
Identity theft: **70%**
Phishing: **64%**
Credit card fraud: **58%**

### Puerto Rico
Identity theft: **80%**
Credit card fraud: **78%**
Account takeover: **57%**

### South Africa
Identity theft: **63%**
Credit card fraud: **62%**
Phishing scams: **48%**

### Spain
Credit card fraud: **66%**
Identity theft: **61%**
Phishing: **49%**

### United Kingdom
Identity theft: **53%**
Credit card fraud: **49%**
Phishing: **39%**

### United States
Identity theft: **59%**
Credit card fraud: **56%**
Account takeover: **36%**

TransUnion

# Consumers continue to demand more from digital experiences

Companies across industries are optimizing digital operations to circumvent sophisticated fraud tactics; provide equitable access to services; and streamline customer experience (CX), acquisition and retention. TransUnion surveyed adults living in 15 international markets to gain insight into consumer attitudes toward digital transactions and fraud.

Globally, almost two in three (62%) consumers said they're likely to switch companies for a better digital experience. Gen Z and Millennials were universally more likely to switch than older generations, while in India, an overwhelming 93% of respondents were likely to do so – by far the highest percentage among markets surveyed. To meet rising consumer expectations, businesses need to focus on offering easy, secure, mobile-first experiences.[1]

## 62% (nearly two-thirds) of consumers would switch companies for a better digital experience

TransUnion

## Easy consumer experiences

Over 60% of consumers told us they abandoned an online application or form before completing it. And over half (52%) of consumers abandoned applications that requested too much information. In this scenario, consumers may either have expected an easier application process or were unable to verify their identity due to having a thin credit file with little or no credit history. These insights suggest digital experiences are potentially falling short, and better identity solutions could offer an opportunity to serve consumers and help improve financial inclusion – a topic we explore later in the report.[1]
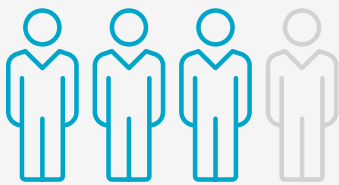
Over three-quarters of consumers prioritized ease of registration when setting up a new account, and 89% said ease of login authentication experience is important when choosing whom to transact with online.

**Consumers value a smooth, friction-right experience at account creation and login. When asked about the most attractive features of online transactions:**

**88%** of consumers prioritized ease of registration[1]

**89%** said ease of login and authentication is important when choosing whom to transact with online[1]

To meet these expectations, a range of authentication solutions can be utilised to provide access across a wider range of consumer preferences and differences in access to technology. These could include options that can be used either online or offline, such as one-time passcodes (OTP) that enable straightforward and effective authentication, or knowledge-based verification. To add a low-friction, two-factor authentication flow, consider methods like device-based authentication that pairs known devices with accounts for fast, smooth logins without the need for passwords.

TransUnion

## Secure experiences

Consumers want strong security processes, like OTP and multifactor authentication, and are ready to drop an application or digital service if they don't trust the provider.

**43%** of global consumers abandoned an online application or form because they didn't think their personal data was secure, while nearly two-thirds (63%) indicated they wouldn't return to a website if they had fraud concerns.[1]

**78%** of respondents globally wanted to be highly confident their personal data would not be compromised before choosing whom to transact with online – showing the perception of fraud risk can sway a consumer's decision when selecting a digital service.[1]

In every market except India, confidence in personal data security was the most important criterion for consumers choosing whom to transact with online – followed by an easy payment process. Respondents in India prioritized ease of new account registration (84%) when choosing whom to transact with online.

**42%** of global consumers said they were targeted by digital fraud in the last three months[1]

TransUnion

## Features that influence consumer decision making online

**Figure 5: What features are very important to consumers when transacting online?** [1]

(Top 2 responses by region)

### Global
Confidence that my personal data will not be compromised
## 78%
Easy payment process
## 69%

### Brazil
Confidence that my personal data will not be compromised
## 87%
Easy payment process
## 72%

### Canada
Confidence that my personal data will not be compromised
## 74%
Easy payment process
## 57%

### Chile
Confidence that my personal data will not be compromised
## 83%
Easy payment process
## 74%

### Colombia
Confidence that my personal data will not be compromised
## 89%
Easy payment process
## 80%

### Dominican Republic
Confidence that my personal data will not be compromised
## 87%
Easy payment process
## 82%

### Hong Kong
Confidence that my personal data will not be compromised
## 65%
Site navigation
## 36%

### India
New account setup/ Ease of registration
## 84%
Easy payment process
## 75%

### Kenya
Confidence that my personal data will not be compromised
## 93%
Easy payment process
## 87%

### Mexico
Confidence that my personal data will not be compromised
## 84%
Easy payment process
## 75%

### Philippines
Confidence that my personal data will not be compromised
## 91%
Easy payment process
## 84%

### Puerto Rico
Confidence that my personal data will not be compromised
## 90%
Easy payment process
## 81%

### South Africa
Confidence that my personal data will not be compromised
## 89%
Easy payment process
## 83%

### Spain
Confidence that my personal data will not be compromised
## 70%
Easy payment process
## 57%

### United Kingdom
Confidence that my personal data will not be compromised
## 67%
Easy payment process
## 55%

### United States
Confidence that my personal data will not be compromised
## 76%
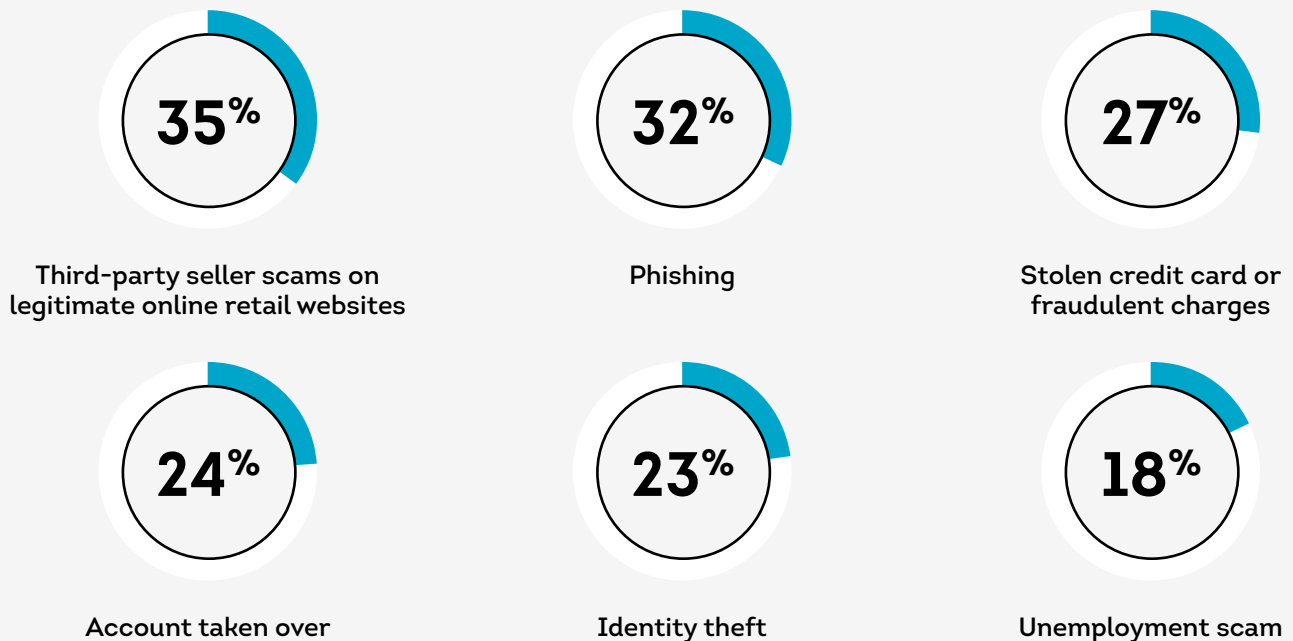Easy payment process
## 63%

TransUnion

## Mobile security concerns

Over 7 billion people used mobile devices worldwide in 2021. That number is projected to reach 7.49 billion by 2025.[3] Downloads in finance apps (covering banks, investments and trading) during 2020 increased 45% worldwide (excluding China), reaching 4.6 billion – with time spent in business apps up 2.75x in a single quarter during 2021.[4]

Despite consumer adoption of mobile and businesses investing money into app development, nearly two-thirds of survey respondents indicated they had been deterred from opening a new online account on the mobile web or in native apps because of security concerns. In terms of generational splits, again there was a pattern of younger generations having higher expectations of the security of mobile experiences than is being offered.

**Figure 6: Consumer experiences with fraud types** [1]

Most frequent fraud schemes global consumers said they were targeted with between Oct. 2021 and Jan. 2022

**35%**

Third-party seller scams on legitimate online retail websites

**32%**

Phishing

**27%**

Stolen credit card or fraudulent charges

**24%**

Account taken over

**23%**

Identity theft

**18%**

Unemployment scam

This reflects the underlying concern consumers have for the security of their personal data during transactions, regardless of channel or device type. The fact that a third of consumers we surveyed who had been targeted by fraudsters had encountered third-party seller scams on legitimate online retail websites, and 23% had been targeted by an identity theft scheme, is likely to be heightening fears and security expectations on digital channels.
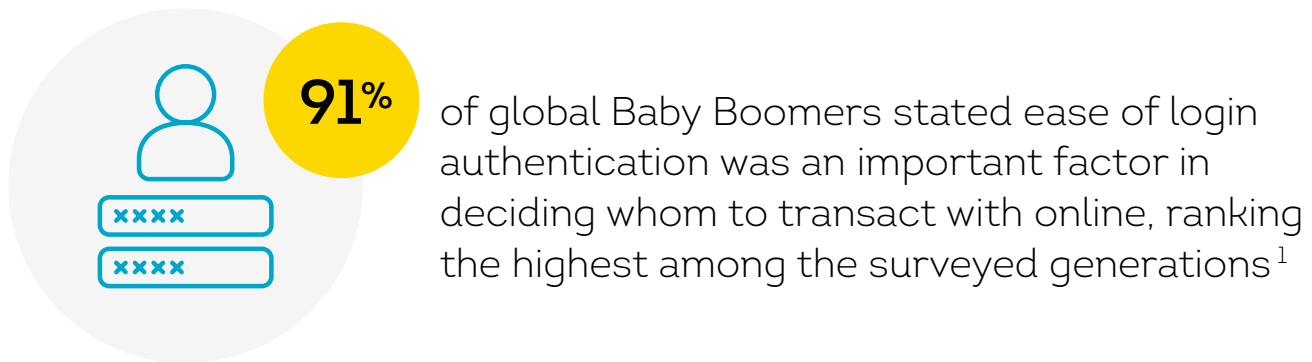
TransUnion

# Next steps: Build trust, improve CX and counter evolving fraud threats

These trends and insights highlight potential business opportunities to optimize identity solutions to help better detect and protect against fraud risks – while simultaneously strengthening consumer experience (CX) and supporting growth opportunities.

## Deploy multilayered protection solutions

We reviewed preferred authentication methods by generation and region (see Figure 7). The findings point toward the fact organizations need a variety of authentication methods for various circumstances and audiences. These methods need to work collectively, which can be difficult if being pulled together from multiple, siloed vendors.

**91%** of global Baby Boomers stated ease of login authentication was an important factor in deciding whom to transact with online, ranking the highest among the surveyed generations[1]

Successful, multilayered identity solutions incorporate a range of checks to deliver a friction-right experience; non-intrusive, robust checks can speed up processes. Innovations, such as facial recognition or document verification, can add friction but when executed correctly, can also speed up processes or help a business position themselves as customer friendly. Multilayered identity solutions help businesses create the type of secure and trusting digital experience consumers crave.

Another important area the research points to is authentication preferences may simply boil down to the technology consumers have access to; as illustrated in figure 7. Regardless of how fast digital transformation has accelerated, there are still significant populations that don't have a smart phone or Internet access, or may prefer to do business face to face. A Gartner Maverick* Research paper[5] explored the risk of businesses leaving consumer segments behind by thinking only digitally. It stressed the need to think holistically about delivering services that cater to different consumer groups. The danger if we don't think this way is it will exacerbate issues such as financial inclusion and further widen the social divide.

TransUnion

**Figure 7: What is your preferred method for verifying your identity when opening a new online account?** [1]

## Global

**Gen Z:** Document verification

**Millennials:** One-time passcodes

**Gen X:** One-time passcodes

**Baby Boomers:** One-time passcodes

### Brazil
**Gen Z:** Biometrics
**Millennials:** Biometrics
**Gen X:** Biometrics
**Baby Boomers:** Biometrics

### Canada
**Gen Z:** Multifactor authentication
**Millennials:** Multifactor authentication
**Gen X:** Multifactor authentication
**Baby Boomers:** Knowledge-based verification

### Chile
**Gen Z:** One-time passcodes
**Millennials:** One-time passcodes
**Gen X:** One-time passcodes
**Baby Boomers:** One-time passcodes

### Colombia
**Gen Z:** Knowledge-based verification
**Millennials:** One-time passcodes
**Gen X:** Knowledge-based verification
One-time passcodes (tied)
**Baby Boomers:** One-time passcodes

### Dominican Republic
**Gen Z:** One-time passcodes
**Millennials:** One-time passcodes
**Gen X:** One-time passcodes
Document verification (tied)
**Baby Boomers:** One-time passcodes
Token-based authentication (tied)

### Hong Kong
**Gen Z:** Biometrics
**Millennials:** Multifactor authentication
**Gen X:** Multifactor authentication
**Baby Boomers:** Multifactor authentication

### India
**Gen Z:** Document verification
**Millennials:** Document verification
**Gen X:** Document verification
**Baby Boomers:** Document verification

### Kenya
**Gen Z:** Document verification
**Millennials:** One-time passcodes
**Gen X:** Knowledge-based verification
**Baby Boomers:** One-time passcodes

### Mexico
**Gen Z:** One-time passcodes
**Millennials:** One-time passcodes
**Gen X:** Multifactor authentication
**Baby Boomers:** Multifactor authentication

### Philippines
**Gen Z:** Document verification
**Millennials:** Document verification
**Gen X:** Document verification
**Baby Boomers:** Document verification

### Puerto Rico
**Gen Z:** One-time passcodes
**Millennials:** One-time passcodes
**Gen X:** One-time passcodes
**Baby Boomers:** Knowledge-based verification

### South Africa
**Gen Z:** Document verification
**Millennials:** One-time passcodes
**Gen X:** One-time passcodes
**Baby Boomers:** Token-based authentication

### Spain
**Gen Z:** Document verification
**Millennials:** One-time passcodes
Multi-factor authentication (tied)
**Gen X:** One-time passcodes
**Baby Boomers:** One-time passcodes

### United Kingdom
**Gen Z:** One-time passcodes
**Millennials:** One-time passcodes
**Gen X:** One-time passcodes
**Baby Boomers:** One-time passcodes

### United States
**Gen Z:** One-time passcodes
**Millennials:** Multifactor authentication
**Gen X:** Multifactor authentication
**Baby Boomers:** Multifactor authentication

TransUnion

## Harness differentiated insights to help grow your customer base

Extra data insights that help better identify consumers support other business initiatives, such as financial inclusion. Over 1 billion adults in the world lack access to basic financial services.[6] Expanding access to credit to underserved communities can unlock more financial services for consumers, which increases potential business opportunities that support greater economic growth.

For some demographics, it's difficult to prove they're who they say they are. For example, in the UK, current identity frameworks often rely on triangulation via proof of name, address and date of birth. Consumers who do not live at a fixed address will struggle to open a bank account or access services.

# Over 1 billion
adults in the world lack access
to basic financial services.

The evolution of a digital trust framework and more holistic use of data offers an opportunity to verify consumer identities with greater confidence. Enhanced credit risk decisions with alternative and trended credit data make services more inclusive while mitigating fraud risk. Alternative data contains information not typically enclosed in traditional sources, whilst trended credit data gives a deeper, broader view of consumers and their behaviours.

An example of the advantage this can offer comes from students; digital natives more likely to have a thin credit file and who may want to present their identity digitally. They have more transient data in their residential data, so their digital footprint is a good anchor point to prove they are who they say and are. This example illustrates how forward-thinking regulation and differentiated insights can securely authenticate a customer and help improve access to digital services and open up new markets.

TransUnion
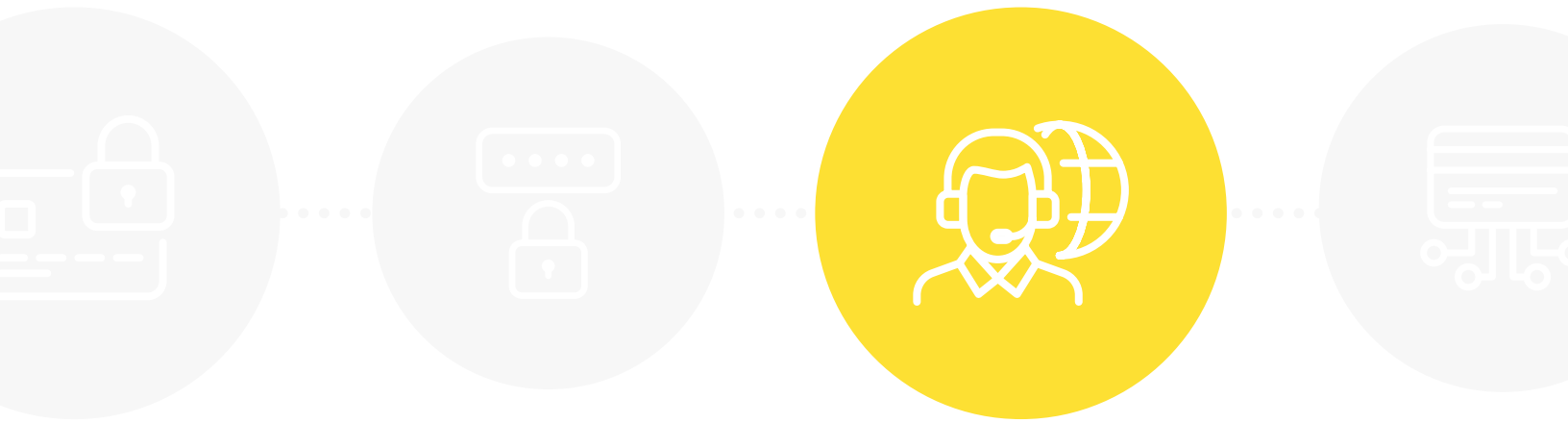
## Take an omnichannel approach to fraud prevention and customer service

Expanding our thinking beyond digital for a moment, consumers increasingly expect smooth, cohesive brand interactions across channels, moving between apps, websites, and call centers to achieve their goals. Bad actors know that call center agents are frequently less protected, despite performing many of the same high-value functions available to consumers via digital channels. A Neustar study found more respondents cited the call center as enabling ATO (account takeover) fraud in 2020 than in prior years. Financial institutions attributed ATO fraud equally to website and call center channels, a change from 2020 when websites took greater blame.[7]

> Financial institutions attributed ATO fraud equally to website and call center channels, a change from 2020 when websites took greater blame.[7]

Engaging callers in authentication – whether by requesting personally identifying information that has been breached or shared on social media, or by comparing a sample of a voice signature to one associated with a customer record – fails to mitigate fraud risk or improve CX.

To identify emerging threats and support omnichannel experiences, forward-thinking organizations assess risk signals about the call and caller. Only risky callers receive additional friction, stepped-up authentication or the full focus of the fraud department. Trustworthy callers experience little-to-no friction and may be offered more valuable self-serve options in the IVR, improving efficiency and CX.

015

7 2021 State of Call Center Authentication Report, Neustar

TransUnion

## Make educational content accessible and easy for consumers to act

We asked consumers what they'd do if they became a victim of digital fraud. Over half (57%) said they'd freeze their credit, while 58% said they'd contact impacted businesses like credit card companies or retailers. Over 40% said they'd place a fraud alert on their credit report. However, when people said they were targeted by digital fraud, only one in three placed a fraud alert on their credit report or set up a credit freeze after being targeted, while 52% indicated they had contacted the impacted company.[1]

Consumers are looking to businesses to help them mitigate fraud and guide them on what to do next. Businesses wanting to lead on this should consider whether the educational content available to consumers effectively instructs them on fraud risks and the ways they can protect themselves, and how accessible the content actually is. Likewise, for fraud victims the priority needs to be ensuring they're able to act easily and quickly using their preferred channel. Empowering consumers so they're informed and motivated to act incrementally helps build trust, brand reputation and minimizes the threat to the bottom line.

When victims of fraud were asked what action they had taken, only one in three said they placed a fraud alert on their credit report

**1 in 3**

## Work with flexible and innovative services

The pandemic highlighted the dynamic nature of fraud threats and rising customer expectations for fast, secure digital services.

Optimization of fraud and identification processes allow insights and risks to be acted upon and processes quickly configured. For example, a single API connection can allow fast and easy integration with existing infrastructure and help you adapt to diverse consumer preferences. This should enable the right solution, such as an ID check, anti-money laundering (AML) check, email verification or document verification, to be delivered at the right moment in the customer lifecycle, thus helping to improve the customer journey. These processes can secure the experience without adding undue friction.

TransUnion

# Conclusion

The trends in this report illustrate the potential threat fraudsters pose, and highlights some of the ways digital identity solutions are likely to influence the nature of fraud risk in the future.

There are, of course, new types of cybercrime just beginning to emerge. We're seeing potential new synthetic fraud risks powered by AI technology, like deepfakes and automated crime, and attempts to corrupt consumer-centric innovations, such as digital wallets and payment types.[8] Media stories related to the boom in cryptocurrencies and NFTs, and how fraudsters are seeking opportunities for illicit gain, are a reminder that whichever direction technology and consumers take, fraudsters will follow. Regulation and necessity for protections will bring these new marketplaces into the orbit of fraud and identity businesses like TransUnion.

We're in an arms race to equip and better protect ourselves, and attempt to close loopholes fraudsters might seek to exploit. It's important to focus on the pivotal role identity can play in delivering an outstanding customer experience whilst lowering your fraud risk and unlocking new growth opportunities. But this is only possible if there's a firm foundation of trust between consumers and businesses.

**Methodology**

This report blends proprietary data from TransUnion's global intelligence network and specially commissioned consumer research.

TransUnion's global intelligence network uses intelligence from billions of transactions originating from over 40,000 websites and apps that use TransUnion TruValidate™ to protect digital transactions. The report represents transactional data analyzed between Jan. 1, 2019 and Dec. 31, 2021. The percent of suspected digital fraud attempts are those that TruValidate customers either denied or reviewed due to fraudulent indicators compared to all transactions it assessed for fraud. The country and regional analyses examines transactions originating from select countries and regions.

TransUnion surveyed 12,500 adults Jan. 12–18, 2022 in partnership with third-party research provider, Dynata. Adults 18 years of age and older residing in 15 countries – Brazil, Canada, Chile, Colombia, the Dominican Republic, Hong Kong, India, Kenya, Mexico, the Philippines, Puerto Rico, South Africa, Spain, the UK and the US.

Survey questions were administered in Chinese (Hong Kong), English, French (Canada), Portuguese (Brazil) and Spanish (Colombia, the Dominican Republic, Mexico, Puerto Rico and Spain). To increase representativeness across resident demographics, the survey included quotas to balance responses to the census statistics on the dimensions of age, gender, household income, race and region. Generations are defined as follows: Gen Z, born 1995–2004; Millennials, born 1980–1994; Gen X, born 1965–1979; and Baby Boomers, born 1944–1964. These research results are unweighted and statistically significant at a 95% confidence level within ±0.88 percentage points based on a calculated error margin.

017

[8] The Art of Cybercrime, Jamie Bartlett, January 2022

TransUnion

# TransUnion®

## Optimize your fraud processes and customer experience

Do you want to unlock the potential of your fraud and identity processes and help lower your fraud risk while enhancing your customer experience? Our innovative data identity solutions and fraud analytics can help businesses uncover new opportunities and adapt to changing dynamics.

Partner with us to improve your customer experience, increase fraud capture rates and drive improvements that could benefit teams across your business.

### About TransUnion

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing an actionable picture of each person so they can be reliably represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things.

**We call this Information for Good.®**

TransUnion Global Fraud Solutions unite both consumer and device identities to detect threats across markets while helping ensure friction-right user experiences. The solutions, all part of the TruValidate™ suite, fuse traditional data science with machine learning to provide businesses unique insights about consumer transactions – safeguarding tens of millions of transactions each day.