TransUnion

TransUnion 2023 State of Omnichannel Fraud Report

Trends and strategies for enabling trusted commerce

Introduction

Globally, in 2022 fraud returned to something more closely resembling pre-pandemic levels. However, with increased digital transaction volumes, the risk to organizations and individuals was even greater than before. Cybercriminals and fraudsters continue to evolve and show increasing sophistication — with stolen identity information at the center of their strategies. Consumers, keenly aware of the risk of using online channels, judge companies based on how well their personal data is protected. Winning organizations will implement smarter fraud prevention strategies that build consumer trust by demonstrating safety in their omnichannel customer experiences.

In the 2023 State of Omnichannel Fraud Report, TransUnion brings together trends, benchmarks and expertise from across our identity and fraud prevention organization. It provides insight and recommendations to those responsible for preventing fraud and streamlining online experiences to deliver better business outcomes. Readers should use this report to evaluate their current fraud prevention programs in the context of the broader market. This information and insight should be shared across the organization with the goal of improving customer satisfaction, reducing fraud and improving business performance.

All data in this report blends proprietary insights from TransUnion's global intelligence network and a specially commissioned TransUnion consumer survey in 18 countries and regions globally.

KEY TAKEAWAYS

Digital growth is driving risk exposure

4.6%
of global digital transactions were potentially fraudulent in 2022

80%
increase in digital transactions resulted in 80% growth in suspected digital fraud attempts globally from 2019 to 2022

Identifiers are being weaponized

83%
increase in publicly reported data breaches in the US from 2020 to 2022

$4.6 billion
outstanding balances attributed to suspected synthetic identities for US auto loans, credit cards, retail credit cards and unsecured personal loans in 2022 (highest level ever and a 27% increase since 2020)

Fraudsters exploit all channels

62%
of high-risk phone calls into US call centers were from non-fixed VoIP phone lines in 2022

52%
of consumers said they were targeted with online, email, phone call or text messaging fraud attempts from Sept. to Dec. 2022

TransUnion

Contents

Global Digital Fraud Trends

Continuing rise in digital transaction volume raises fraud risk

TransUnion determined 4.6% of its customers' digital transactions screened for fraud worldwide were suspected fraudulent attempts in 2022. While this rate returned to its pre-pandemic level, TransUnion measured an 80% increase in global digital transactions among its customers from 2019 to 2022, and a resulting 80% increase in the volume of suspected digital fraud attempts.

This trend was present in many countries we analyzed. For instance, digital transactions originating in the US increased 89% and the volume of suspected digital fraud attempts 122%. This represents a significant increase in fraud exposure for organizations and individuals. Identity and financial fraud represented the highest proportion of digital fraud attempts globally. Synthetic identity fraud rose the fastest (at 76%) among the top five digital fraud types reported to TransUnion by its customers since 2019.

80% increase in the volume of suspected digital fraud attempts globally from 2019 to 2022

Industries targeted follow consumer digital engagement

The pandemic crystallized the fact bad actors focus their efforts on organizations and institutions that have direct access to money, products or services with easily transferable monetary value. While government-funded pandemic relief programs experienced headline-grabbing levels of fraud, digital fraud trends point to industries that saw significant growth in consumer digital engagement.

Fraudsters increased suspected digital fraud attempts targeting travel & leisure, logistics and financial services the most from 2019 to 2022, rising 117%, 63% and 39%, respectively. Each of these industries experienced significant transaction volume increases during this time, as the pandemic drove shifts in consumer behavior.

TransUnion's Digital Fraud Measurement
The rate or percent of suspected digital fraud attempts reflects those which TransUnion customers either denied in real time due to fraudulent indicators or determined were fraudulent after reviewing — compared to all transactions it assessed for fraud.

Global Digital Fraud Attempts by Industry 2022

Suspected fraud attempt rate 2022 | Top fraud type 2022 | Suspected fraud attempt rate percentage change 2019–2022

Gaming
(online sports betting, poker, etc.)

2022
7.5%
Promotion abuse

2019-2022
-21%

Retail

2022
7.2%
Promotion abuse

2019-2022
7%

Video gaming

2022
5.4%
Gold farming

2019-2022
-82%

Financial services

2022
4.2%
True identity fraud

2019-2022
39%

Communities
(online dating, forums, etc.)

2022
4.0%
Profile misrepresentation

2019-2022
-8%

Travel & leisure

2022
2.1%
Credit card fraud

2019-2022
117%

Telecommunications

2022
2.1%
Credit card fraud

2019-2022
-51%

Insurance

2022
1.7%
Third-party fraud

2019-2022
22%

Logistics

2022
1.3%
Shipping fraud

2019-2022
63%

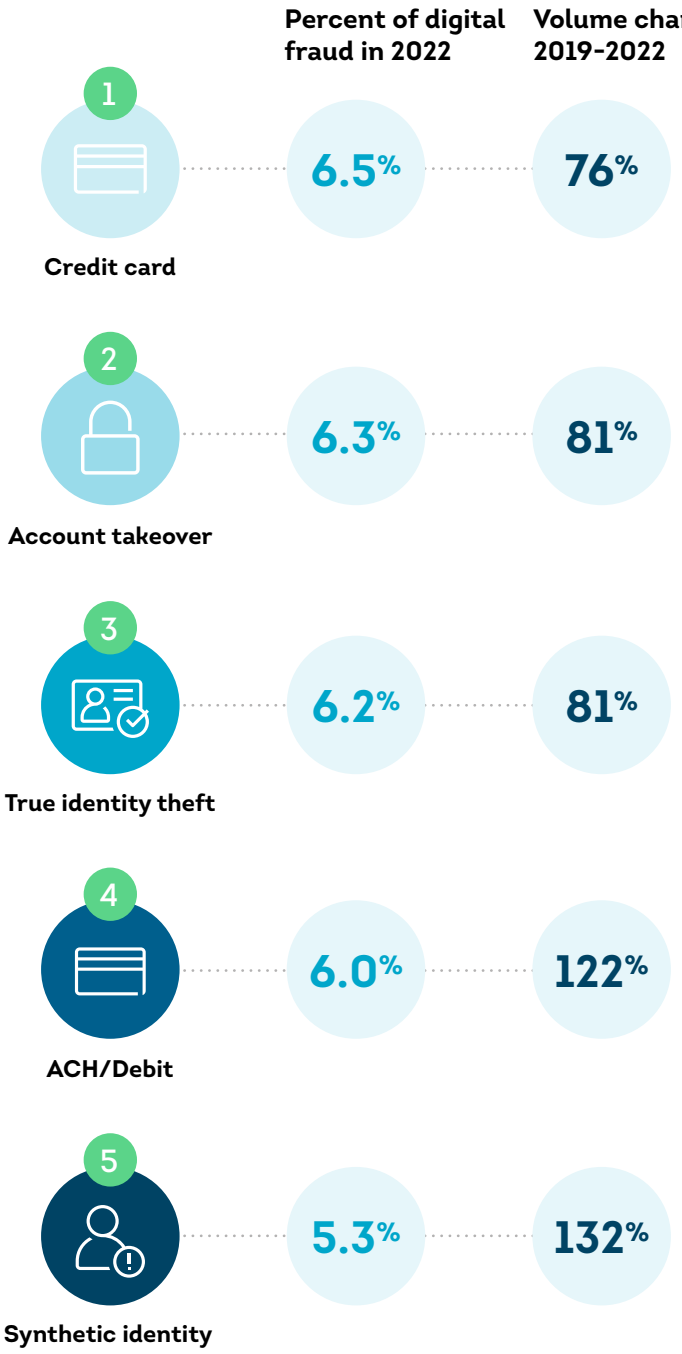
Source: TransUnion TruValidate

TransUnion

Identity-based fraud growth increases risk for consumers and businesses

The increasing sophistication of fraudsters was evident in the growth of certain types of fraud. Identity theft and identity scams — such as phishing, vishing and smishing which aim to accumulate identity information — drove increases in stolen identities and resulted in account takeovers, payment frauds and the creation of new accounts with fabricated/misrepresented or synthetic identities.

Top Fraud Types and Their Growth



Source: TransUnion TruValidate

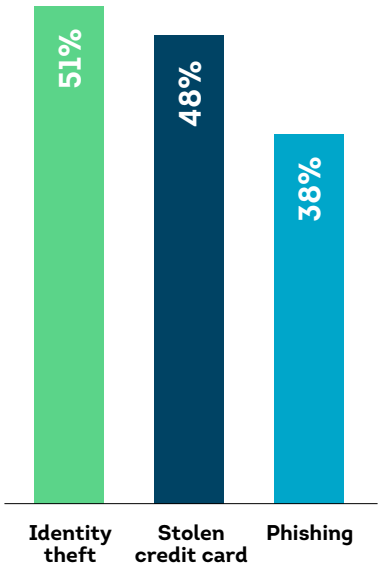
Consumers are aware their identities are at risk

As mentioned previously, digital transactions observed by TransUnion nearly doubled over the last four years. With the increased use and dependence on digital channels, consumers are concerned with identity theft and digital fraud. While the top fraud concern differs by country or region, consumer unease about their identities being compromised is universal.

Top Consumer Fraud Concerns by Country and Region

Percentage who said they were concerned with falling victim to the following types of fraud

UNITED STATES



BRAZIL

Vishing: **69%**
Identity theft: **57%**
Phishing: **51%**

CANADA

Identity theft: **57%**
Stolen credit card: **56%**
Phishing: **46%**

CHILE

Vishing: **72%**
Phishing: **64%**
Identity theft: **58%**

COLOMBIA

Vishing: **70%**
Phishing: **69%**
Identity theft: **61%**

DOMINICAN REPUBLIC

Vishing: **76%**
Phishing: **73%**
Stolen credit card: **57%**

HONG KONG

Vishing: **58%**
Phishing: **53%**
Identity theft: **49%**

INDIA

Phishing: **38%**
Third-party seller scam: **36%**
Identity theft: **35%**

KENYA

Phishing: **59%**
Account takeover: **58%**
Identity theft: **58%**

MEXICO

Vishing: **68%**
Phishing: **59%**
Identity theft: **49%**

NAMIBIA

Account takeover: **69%**
Identity theft: **65%**
Stolen credit card: **64%**

PHILIPPINES

Phishing: **67%**
Identity theft: **63%**
Third-party seller scam: **58%**

PUERTO RICO

Phishing: **69%**
Identity theft: **67%**
Vishing: **67%**

RWANDA

Third-party seller scam: **42%**
Account takeover: **38%**
Stolen credit card: **37%**

SOUTH AFRICA

Identity theft: **62%**
Stolen credit card: **57%**
Account takeover: **55%**

SPAIN

Vishing: **62%**
Phishing: **56%**
Smishing: **49%**

UNITED KINGDOM

Identity theft: **52%**
Stolen credit card: **45%**
Account takeover: **41%**

ZAMBIA

Account takeover: **67%**
Identity theft: **64%**
Third-party seller scam: **63%**

Source: TransUnion consumer fraud survey

Data Breach Trends

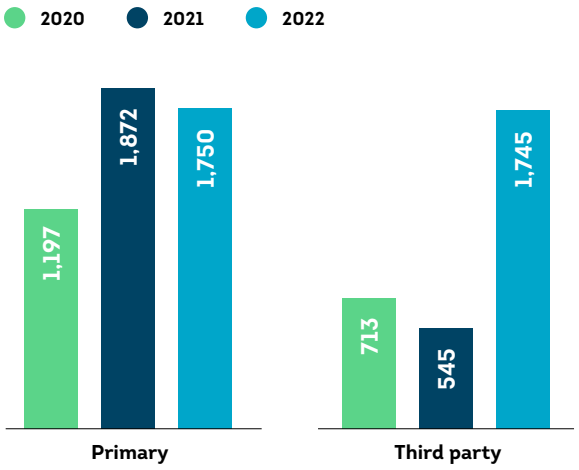
US data breaches increase in volume and severity – a leading indicator of future fraud

Based on publicly available data analyzed by Sontiq, a TransUnion company, the number of data breaches in the US increased 83% from 2020 to 2022 (1,910 in 2020; 2,417 in 2021; and 3,495 in 2022). In addition, from 2020 to 2022, the severity of data breaches, as measured by Sontiq's Breach Risk Score (BRS), increased 6%.

The rise of third-party breaches

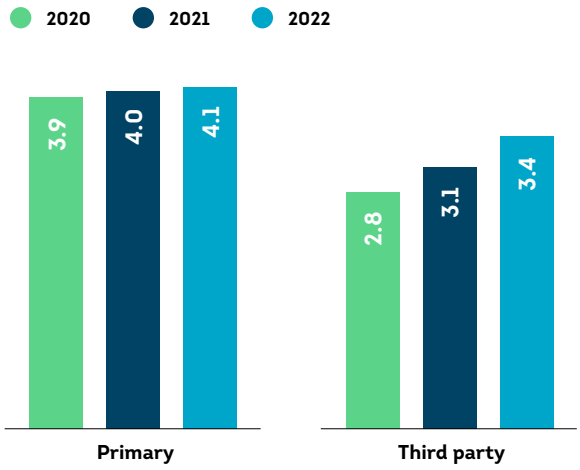
Sontiq also determined the number of breaches with third parties rose 145% from 2020 to 2022. A third-party attack, also known as a supply-chain attack, value-chain attack or backdoor breach, is when an attacker accesses an entity's network via third-party vendors or suppliers — payroll processing or medical billing, for instance. The BRS for third-party breaches also increased 23% compared to 4% for primary business breaches. In the future, businesses will likely be impacted by a greater number of and more sophisticated fraud attacks, while consumers will experience heightened risk to their financial well-being.

US Data Breach Volume 2020–2022 by Primary and Third Party



Source: Sontiq, a TransUnion company

Average Breach Risk Score for US Data Breaches



Source: Sontiq, a TransUnion company

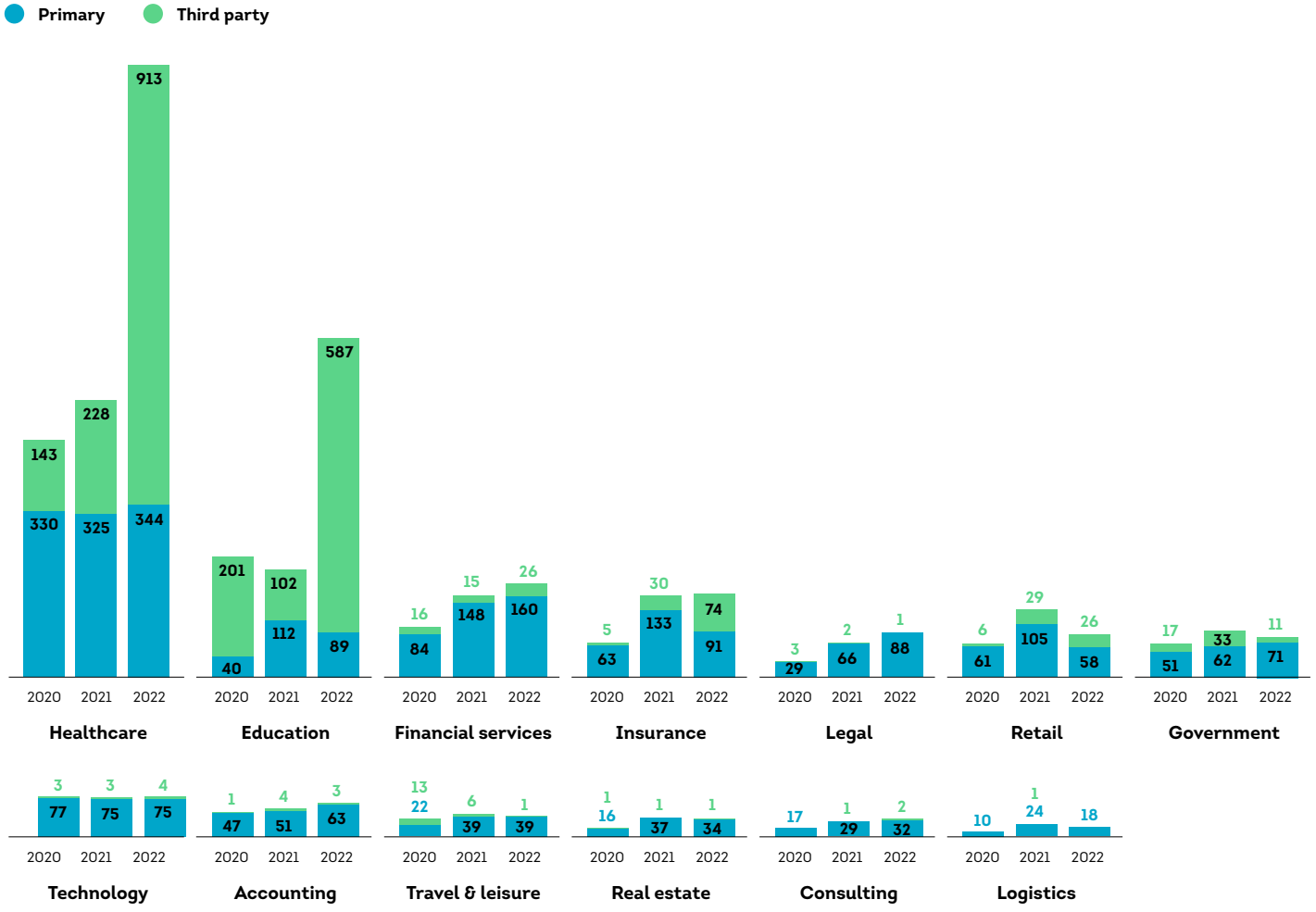
Sontiq's Breach Risk Score (BRS) is purely based on the quantity and severity of the particular ID credentials the affected entity determined to have been exposed. From among 60 possible ID credential choices, each is run through BreachIQ™ (Sontiq's 1,300-element, AI algorithm) to produce a risk score and pattern, and prescribed consumer actions. The Breach Risk Score uses a 1–10 scale: 1 represents least severe and 10 represents most severe. To check the BRS for a specific breach and see steps Sontiq recommends consumers take, go to **sontiq.com/breachiq/#search-breached-organizations**.

Data breaches fuel identity engineering, impacting all industries

As data breaches increase in both volume and severity, it's critical to differentiate the risk certain types of breaches have on fraud prevention strategies. Cybercriminals have significant basic identity data available via the dark web, yet relatively fewer of the most essential ID credentials — such as government identifiers or financial account numbers — are found there. Industries experiencing the greatest data breach growth appear to be targeted for their identity data that fraudsters use to create synthetic identities or facilitate more sophisticated social engineering attacks. For instance, by accessing personal data, fraudsters have the information they need to gain access to financial services accounts like banks and credit cards, drain money there and then use that financial account information to make purchases in other industries.

Healthcare produced the most breaches of any single industry: more than 1,250 in 2022 and nearly 2,300 over the past three years, representing 36% and 29% of all US data breaches, respectively. Not only did healthcare experience the most breaches, it also tied with the legal and logistics industries for the most severe breaches in 2022 with an average BRS of 4.7. Other sectors that had severe breaches included accounting (4.6), real estate (4.6) and financial services (4.4) — many of which were smaller firms lacking the security infrastructure and procedures to protect their networks.

US Data Breaches by Industry, Primary and Third Party



Source: Sontiq, a TransUnion company

Global Consumer Fraud and Customer Experience Sentiment

Customer experience that honors identity protection is a winning strategy

Globally, 36% of consumers surveyed by TransUnion reported conducting more than half of their transactions online. That said, they clearly understand the risks of doing business online and beyond; more than half reported being targeted by fraudsters from Sept. to Dec. 2022.

Consequently, consumers value organizations that protect their identities and online accounts. Those that don't honor these preferences may lose business; more than half (59%) of consumers reported they'd switch companies to get a better digital experience.

Security and fraud concerns inhibit digital commerce

63%
would not return to a website due to fraud concerns

55%
have been deterred from opening an account on a mobile device due to security concerns compared to 48% for desktop devices

48%
abandoned their online shopping carts due to fraud and/or security concerns

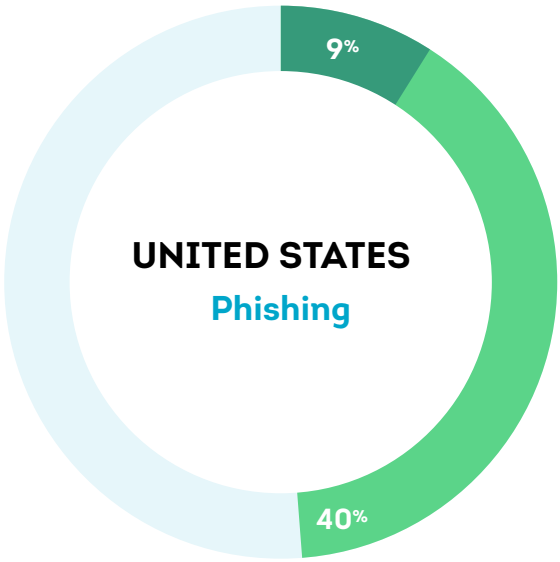
Source: TransUnion consumer fraud survey

Consumers face identity attacks regularly

More than half (52%) of respondents reported being targeted by email, online, phone call or text messaging fraud from Sept. to Dec. 2022, with 9% becoming victims. Consumers in Africa reported some of the highest fraud rates: 81% of Kenyans said they'd been targeted, and 14% of South Africans fell victim. Globally, most regions reported their most frequently experienced fraud attacks were some type of social engineering scam like phishing, vishing or smishing.

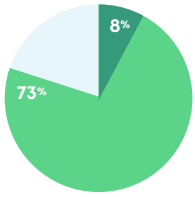
Reported Email, Online, Phone Call or Text Messaging Fraud from Sept. to Dec. 2022 by Country and Region

- Targeted but didn't fall victim
- Targeted and fell victim
- Most reported fraud scheme
- Not targeted



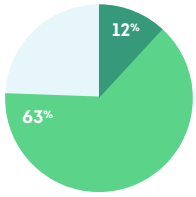
UNITED STATES
Phishing

KENYA



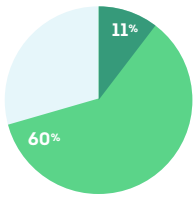
Vishing

ZAMBIA



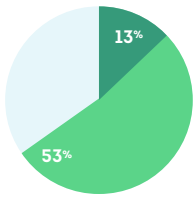
Smishing

PHILIPPINES



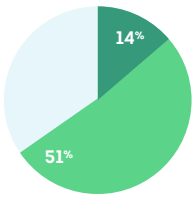
Phishing

NAMIBIA



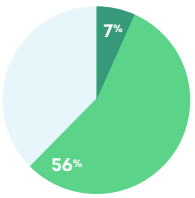
Phishing

SOUTH AFRICA



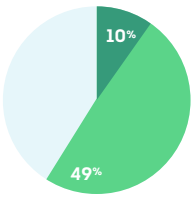
Smishing

RWANDA



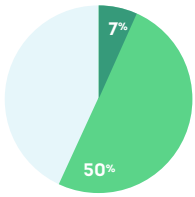
Money mule and third-party seller scam

INDIA



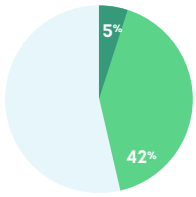
Phishing

CANADA



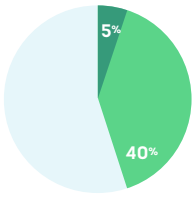
Phishing

UNITED KINGDOM



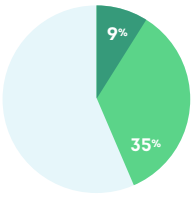
Phishing

HONG KONG



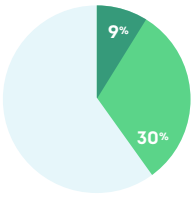
Phishing

PUERTO RICO



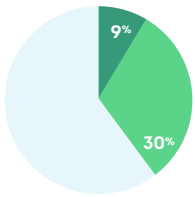
Vishing

BRAZIL



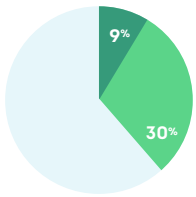
Stolen credit card

MEXICO



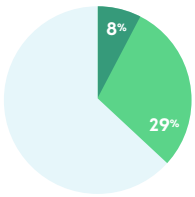
Stolen credit card

CHILE



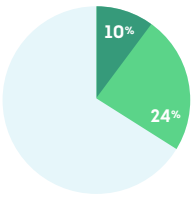
Vishing

COLOMBIA



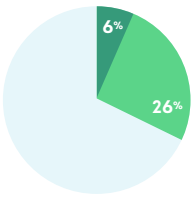
Vishing

DOMINICAN REPUBLIC



Stolen credit card

SPAIN



Phishing

Source: TransUnion consumer fraud survey

TransUnion

Consumers prefer businesses that protect their personal data

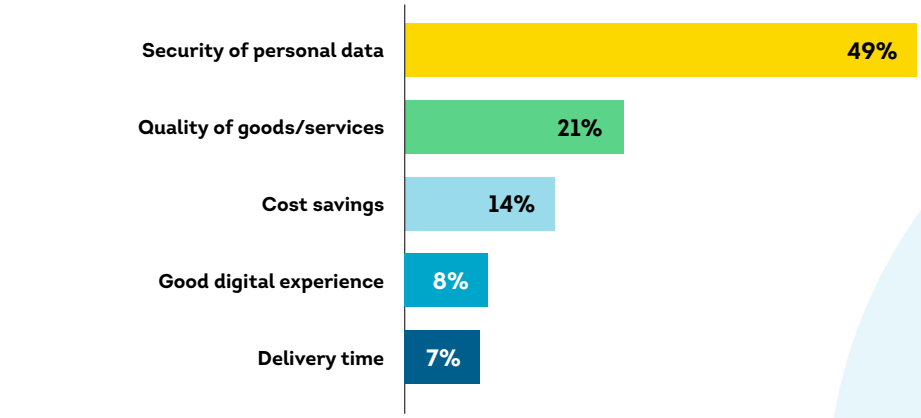
Given how regularly consumers experience potential fraud, they value organizations that instill confidence their personal data will be protected. Most (78%) respondents said they prefer organizations whose online experiences protect personal data. Additionally, 49% of consumers ranked security of personal data as the number one quality or expectation when deciding what online company to do business with. That's more than twice that of quality goods and services (21%) and three times that of cost savings (14%).

Stated Important Features When Choosing Who to Transact With Online

Very important

Ranked Expectations or Qualities in Preferred Online Companies

Top answer chosen



Source: TransUnion consumer fraud survey

TransUnion

Implications for Fraud Prevention Leaders

Reduce friction to increase conversion rates

The knee-jerk response to rising data breaches and persistent digital fraud might be to increase identity verification and authentication checks. However, the transition to an always-on, digital-first customer experience, evidenced by the dramatic increase in digital transactions over the past few years, means fraud leaders must be aware of customer experience and enable the business to drive top-line growth while reducing fraud risk.

Business performance means converting more sales — more prospects to customers and more transactions for existing customers. This requires reducing friction for prospects and customers alike. Regardless of the conversion point, reducing friction for consumers provides increased confidence and convenience – confidence they can trust the business will protect their personal data and deliver the hassle-free digital experience they're looking for.

Unfortunately, a lot of consumers don't gain confidence or experience convenience from the businesses they engage. More than half (53%) of consumers reported abandoning an online application or form for a financial or insurance product, with 42% indicating they did so due to personal data security concerns. Additionally, 48% abandoned their shopping carts due to fraud and/or security concerns. To increase conversion rates and reduce transaction friction, business leaders should consider two strategies.

Strategy to increase conversion rates:

- Improve ability to instill trust for new users

Strategy to reduce friction:

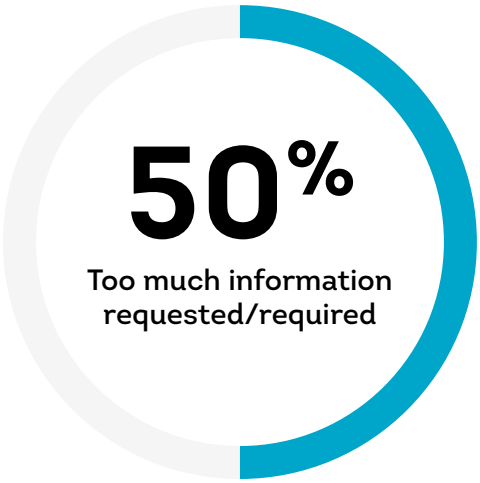
- Align online account authentication with consumer preferences

53%

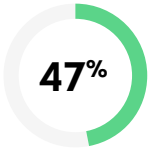
reported abandoning an online application or form for a financial or insurance product

Top Reason Consumers Said They Abandoned Online Application or Form For a Financial or Insurance Product

UNITED STATES



BRAZIL

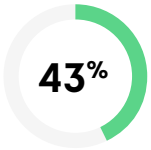


Didn't trust personal data would be secure

CANADA

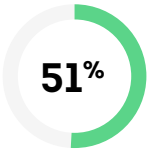
Too much information requested/required

CHILE



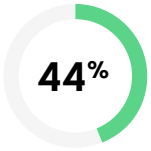
Didn't trust personal data would be secure

COLOMBIA



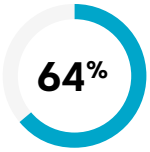
Didn't trust personal data would be secure

DOMINICAN REPUBLIC



Didn't trust personal data would be secure

HONG KONG

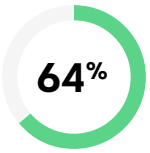


Too much information requested/required

INDIA

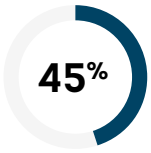
Too much information requested/required

KENYA



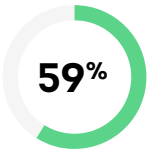
Didn't trust personal data would be secure

MEXICO



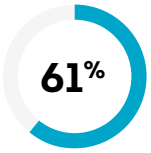
Site too slow

NAMIBIA



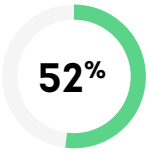
Didn't trust personal data would be secure

PHILIPPINES



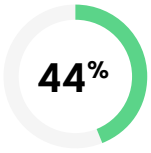
Too much information requested/required

PUERTO RICO



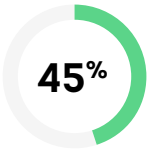
Didn't trust personal data would be secure

RWANDA



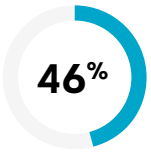
Didn't trust personal data would be secure

SOUTH AFRICA



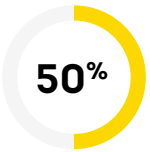
Didn't trust personal data would be secure

SPAIN



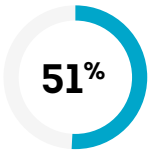
Too much information requested/required

UNITED KINGDOM



Process was frustrating

ZAMBIA



Too much information requested/required

Source: TransUnion consumer fraud survey

TransUnion

Strategy to increase conversion rates: Improve ability to instill trust for new users

It's easy to imagine a consumer would abandon a website that didn't utilize encryption — evidenced by a padlock icon in their browser's address field — especially when providing personal data. And for the most part, for a legitimate business, providing that level of security is table stakes.

The identity verification process required to protect the consumer and your business is more nuanced but no less critical to instilling trust. Identity verification is imperative given consumers around the world reported a willingness to modify their digital identities when establishing new accounts or applying for credit. This could be as simple as using a newly created email address, reporting living at an old address or altering one's name slightly.

Top ways consumers would modify their identity attributes when signing up for a service

31%
Create and use a new email

22%
Create and use a new phone number

19%
Purposefully use different variation of name

18%
Use a different address than the one they reside at

Source: TransUnion consumer fraud survey

Compound this consumer behavior with altered or synthetic identities generated by fraudsters and organizations can be overwhelmed by disconnected digital attributes that make it difficult to verify an individual's identity, necessitating additional layers of identity verification friction.

To overcome these complexities, fraud prevention teams should utilize an identity graph with strong foundational identity data and robust identity resolution capabilities. By tying together multiple digital attributes like devices and accounts a single consumer uses, organizations can be confident they know who they're engaged with and continue to minimize friction throughout the consumer's transaction.

Next steps

To increase confidence in consumer identities to reduce the need for additional verification, fraud managers should utilize an identity graph. Use a solution that provides access to robust offline and online identity attributes like name, terrestrial address, email address and phone number. That identity data, artificial intelligence and machine learning (AI/ML) can be combined in an identity graph that continuously connects relevant identity attributes. Leveraging identity graph technology for identity verification can help streamline new customer conversions while reducing additional verification steps in the first critical moments of the user experience.

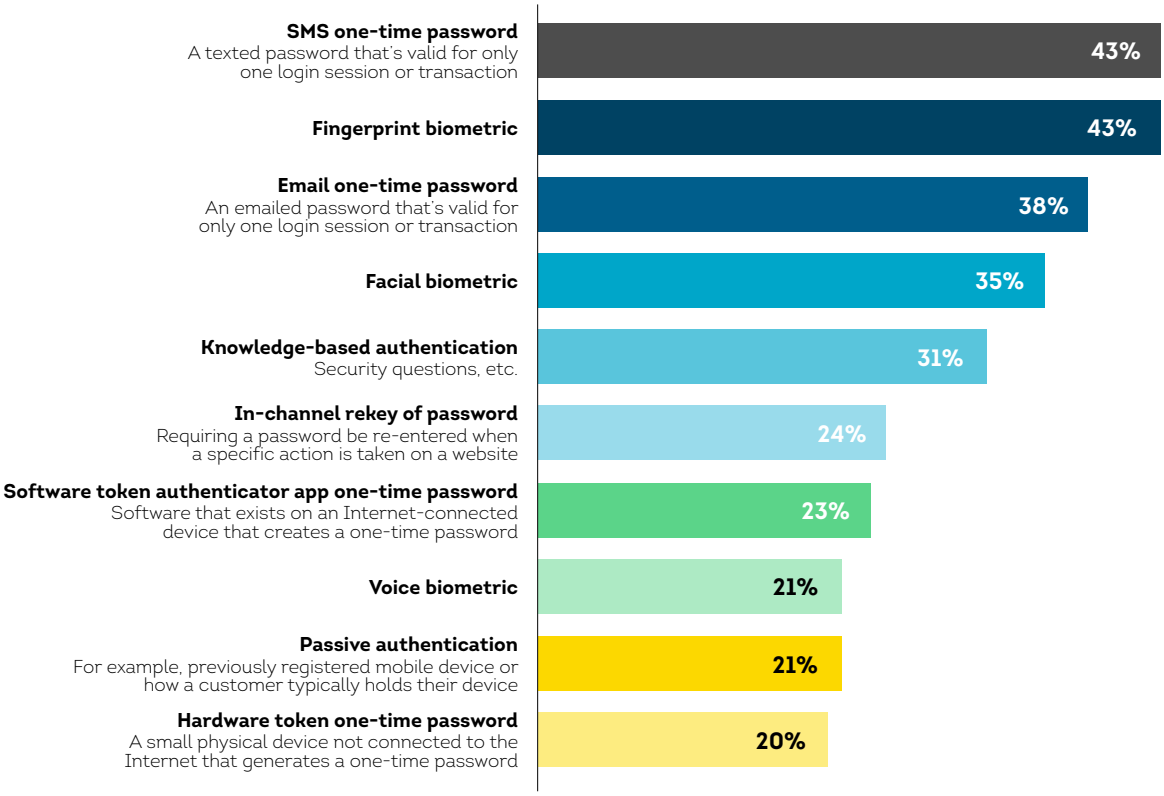
Strategy to reduce friction: Align online account authentication with consumer preferences

Consumers expect their accounts to be protected. And while they understand protection means they must authenticate themselves, they don't want to be hassled by the authentication process. In fact, 63% of respondents indicated they want to be explicitly authenticated to access their online accounts. Most (70%) preferred to be authenticated once at the start of their online sessions. By contrast, 64% didn't want to be reauthenticated after logging into their accounts, such as when making a payment or changing a password. A clear majority (78%) said they prefer having multifactor authentication turned on all the time.

Fraud managers should listen to consumers and incorporate authentication processes that ensure account integrity. At the same time, they should reduce friction by applying additional authentication only to those accounts with suspicious behavior.

Consumer-Stated Preferred Extra Online Security Measures

Percentage in the top three responses



Source: TransUnion consumer fraud survey

Next steps

Managers should focus on risk-based authentication — continuous assessment of the user session — to interrogate the user further if risk increases. They should implement multifactor authentication like secure one-time passcode OTP (for SMS, ensure evaluation for phone takeover risk), or via app-based push notification and biometric authentication using fingerprint or facial recognition. They might also consider a seamless authentication process facilitated by device-based authentication for high-trust accounts.

63%

of respondents indicated they want to be explicitly authenticated to access their online accounts

REAL-WORLD EXPERIENCE

Enhanced identity verification and authentication reduced application abandonment

Large **global credit card provider** experiencing a 63% drop off in applications due to excess friction. The lender applied a more robust identity verification and authentication processes resulting in:

50%

reduction in fraudulent applications – saving approximately $1.5 million annually

13%

reduction in abandoned applications – leading to over 51,000 new applications submitted with a potential revenue gain of $12.3 million USD

Improve fraud detection while reducing false positives

For fraud managers, false positives that stop good transactions for additional authentication are lose-lose propositions. Not only can additional authentication annoy good customers to the point of them potentially taking their business elsewhere, but also manual reviews are costly and demand resources that could be spent uncovering actual fraud.

Unfortunately for large organizations with many channels, including financial services, government and retail, operations can be siloed with disparate customer data systems. It's likely an existing customer engaging with a new channel or purchasing a new product from another business unit may produce a false positive simply because they're unrecognized. To improve fraud detection while reducing false positives, fraud managers should consider two strategies.

Strategy to reduce false positives:

- Take an omnichannel approach to fraud prevention

Strategy to improve fraud detection:

- Enhance identity verification with device proofing

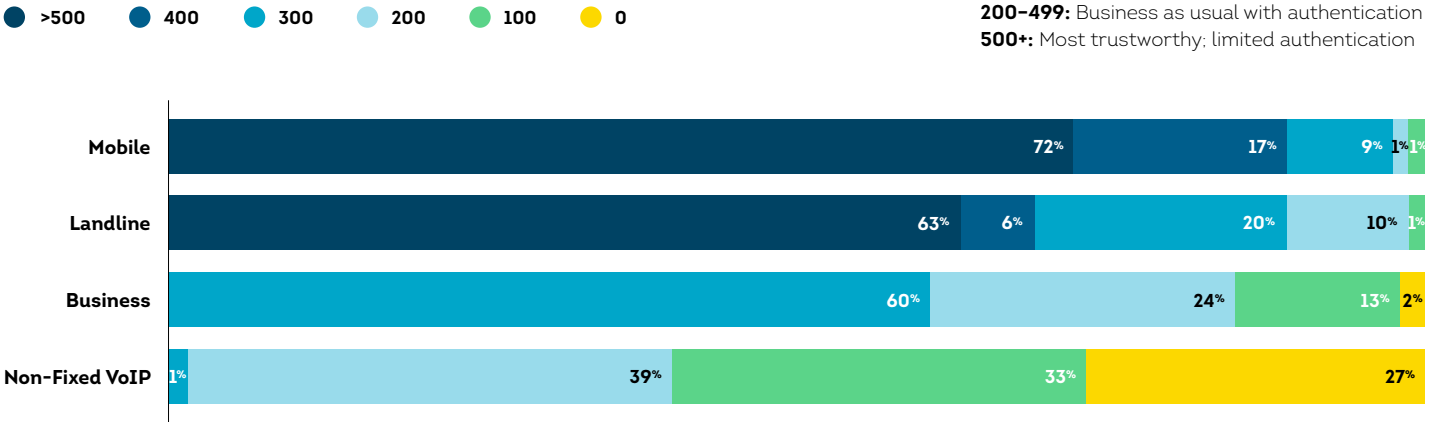
False positives that stop good transactions for additional authentication are lose-lose propositions.

Strategy to reduce false positives: Take an omnichannel approach to fraud prevention

Despite most organizations encouraging customers to manage their account information online, such as changing passwords or updating address information, consumers will use whichever channel is most convenient at the time. To that end, most (60%) survey respondents reported doing less than half of their account management online, with 15% doing none. That means customers use call centers or visit retail locations more frequently for a variety of transactions. It also means fraud prevention managers need to work with teams in every customer channel, including call centers, to break down customer data siloes and ensure a consistent account authentication process is applied regardless of channel.

While TransUnion documented the vast majority (85%) of calls received by its US financial services call center customers were from mobile phones in 2022, less than 2% of those calls were identified as being high risk for fraud, and just 14% of all high-risk calls were made from a mobile phone last year. The riskiest channel for the call center is non-fixed Voice over Internet Protocol (VoIP), a phone number that isn't associated with a physical address. While that channel represented only 3% of total call volume, 60% of those calls were identified as high risk for fraud, and 62% of all high-risk calls came from non-fixed VoIP last year.

US Call Center Risk by Channel and Overall Volume



Call risk score tiers

0–199: Highest; step-up authentication
200–499: Business as usual with authentication
500+: Most trustworthy; limited authentication

Source: TransUnion TruValidate

Next steps

Fraud managers should work with their call center teams to implement integrated inbound call authentication technology based on robust phone and device reputation. This allows customers to seamlessly utilize both call center and digital channels without the risk of being inconvenienced by further scrutiny due to false positives. For call centers, high-risk calls can immediately be routed for additional authentication or to fraud teams. It also allows trusted calls to move through to Interactive Voice Response (IVR) or representatives with little to no additional authentication.

Strategy to improve fraud detection: Enhance identity verification with device proofing

Rising identity-based fraud demands improving all the tools in the fraud prevention toolkit. Using device reputation tracking (aka device fingerprinting) can help in assessing risk to reduce friction and increase conversion. But relying exclusively on device reputation is risky: Fraudsters often cycle through real or emulated devices to thwart the tracking of previously seen devices. Unknown devices may present a question mark to a device fingerprinting solution, leading to an increase in fraud risk, false positives and unnecessary friction. Without additional risk signals, there's no way to determine whether users behind new devices deserve a warm welcome or additional scrutiny.

Using additional risk signals or device proofing determines the trustworthiness of the device and the identity using it before authentication is initiated, reducing the need for additional authentication. Device proofing extends identity verification for digital experiences by assessing the risk of the identity operating the device. Device proofing leverages a multiprong approach to assess risk: device fingerprinting, device-to-identity linkages and user-behavior analysis. It can help reduce false positives for customers using a new device or new customers establishing a new account.

Top identity-based, digital fraud growth – 2019 to 2022

81%
true identity theft

132%
synthetic identity

Source: TransUnion TruValidate

Next steps

Fraud managers should look to reduce false positives by enhancing their fraud programs with device proofing capabilities. Implement these device-based capabilities to allow trusted visitors through while flagging risky visitors for enhanced verification. Look for solutions that include a broad range of device, identity and behavioral metrics that can be applied to your fraud detection model to understand the identity behind the device that's accessing your network.

REAL-WORLD EXPERIENCE

Robust identity verification reduced application fraud

A major **European consumer lender** sought to drive global growth and reduce online application friction. The lender implemented a more robust, device-based identity verification solution resulting in:

40%
reduction in fraudulent applications – saving approximately €16 million annually

Synthetic identities have potential to impact fraud beyond financial services

Financial services fraud and risk managers have focused on combating synthetic identities for years. Synthetics represent real financial risk to bankers and lenders. These modified or fully fictional identities are used to open accounts, build credit histories and access and utilize credit, as well as launder illicit funds. Outstanding balances[1] attributed to synthetic identities for auto, credit card, retail credit card and personal loans in the US were at the highest point ever recorded by TransUnion — reaching $1.3 billion in Q4 2022 and $4.6 billion for all of 2022.

And while synthetic identities have so far been a financial services problem, given the goal of bad actors to use synthetics to build legitimate credit histories, any organization could be at risk of exploitation by cybercriminals.

Strategy: Apply advanced analytics to detect synthetic identities and accounts

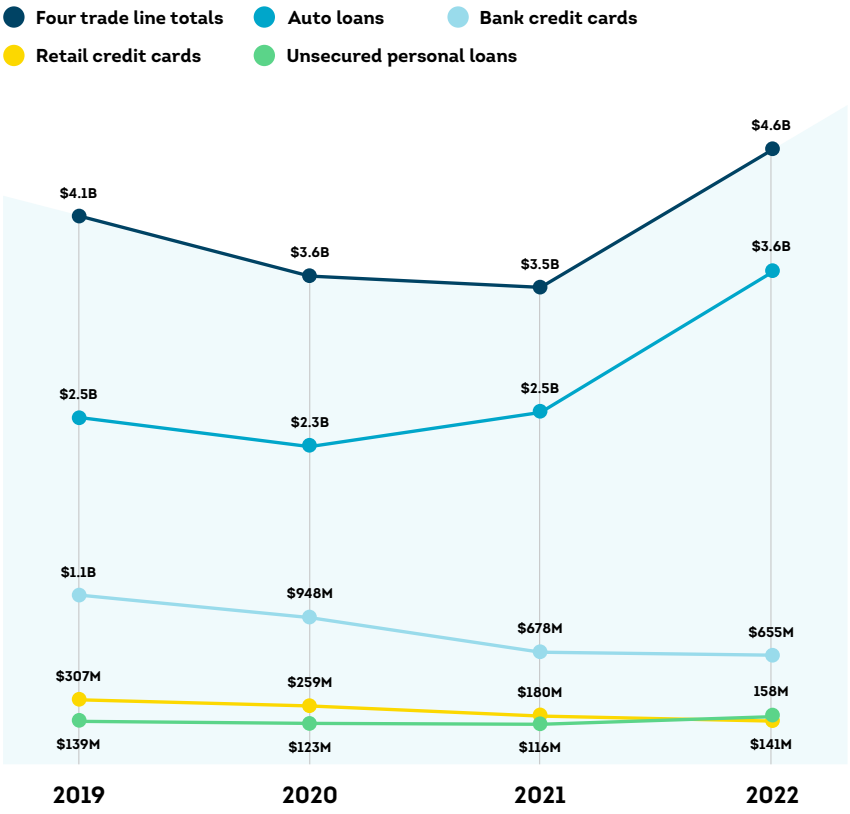
While fraudsters' use of synthetics waned during the pandemic, it's been rising steadily since early 2021. Whether completely fictitious or modified identities, synthetics pose a threat to profits and result in wasted customer acquisition investments. Because they often don't surface until accounts have been charged off, it's important fraud managers stop them from originating — or catch them through account reviews utilizing purpose-built, FCRA-compliant (Fair Credit Reporting Act) synthetic fraud detection models.

US Financial Services Synthetic Identity Incidences for New Credit Accounts Opened

Source: TransUnion TruValidate

1 An outstanding balance is the amount the consumer owes on the obligation as of that date

Outstanding Balances for Suspected Synthetic Credit Accounts in the US



Source: TransUnion TruValidate

Next steps

Leverage fraud detection models purpose built to detect synthetic identities throughout the customer lifecycle. This includes at the point of origination, during credit decisioning and when monitoring existing portfolios. Using dedicated synthetic models also helps deliver prioritized accounts in order of risk to case managers, helping institutions improve compliance for aging inventory and know your customer (KYC) for regulatory reporting deadlines.

Furthermore, in the US, implementing electronic Consent Based Social Security Number Verification (eCBSV) — which allows permitted entities to verify if an individual's Social Security number, name and date of birth combination matches Social Security records — can be an effective and efficient way to prevent synthetic fraud.

REAL-WORLD EXPERIENCE

Synthetic fraud model implementation reduced potential charge offs

Major **US financial institution** sought to protect its online origination and funding business model from synthetic fraud risk. The lender implemented a synthetic fraud model at point of credit decisioning, resulting in:

10%–15%

of potential charge-offs proactively prevented, representing 0.7% estimated reduction in bottom line losses.

Conclusion

Looking forward to 2023 and beyond, fraud prevention leaders must prepare their organizations for ever more sophisticated techniques used by cybercriminals. In a digital-first world, identity data is a vital target for cybercriminals with the means of weaponizing engineered identities for fraud schemes. Building reputable identities is a key goal for these bad actors — using technology to operate with scale and speed.

Consumers, on the other hand, want secure ecommerce platforms where they can transact with confidence. And they want their digital experiences to be convenient at every stage of the customer journey. That said, consumers do want some transaction friction to ensure they're safe — but not so much as to hinder their progress.

It's incumbent upon fraud leaders to take an enterprise-wide approach to fraud prevention and building customer trust. Employ a strategy of continuous innovation through better data, analytics and technology to more accurately detect possible fraud while reducing friction for good customers.

Consumers want secure ecommerce platforms where they can transact with confidence.

Data Sourcing Methodology

This report blends proprietary data from TransUnion's global intelligence network and specially commissioned consumer research. TransUnion TruValidate™ suite comprises identity and fraud products that secure trust across channels and deliver seamless consumer experiences.

Call center

TransUnion's call center findings were based on data from more than a half billion transactions in 2022 — from both large and small financial institutions based in the US. The rate or percentage of high-risk calls was determined by the assessment of multiple risk factors.

Consumer survey

This online survey of 13,383 adults was conducted Dec. 8–23, 2022, by TransUnion in partnership with third-party research provider Dynata. Adults 18 years of age and older residing in 18 countries (Brazil, Canada, Chile, Colombia, the Dominican Republic, Hong Kong, India, Kenya, Mexico, Namibia, the Philippines, Puerto Rico, Rwanda, South Africa, Spain, the UK, the US and Zambia) were surveyed using an online research panel method across a combination of desktop, mobile and tablet devices. 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 ensure representativeness across resident demographics, the survey included quotas to balance responses across key demographics like age, gender and income. Please note some chart percentages may not add up to 100% due to rounding or multiple answers being accepted.

Data breaches

Sontiq, a TransUnion company, obtains its proprietary cyber breach data in partnership with the Identity Theft Resource Center (ITRC). The ITRC staff track a number of sources of all US publicly reported data exposure events from sources that include state Attorneys General, breached entity press releases, law firms, cybersecurity experts and more. Sontiq runs the data through its 1,300-element AI algorithm to produce a risk score, top consumer risks and prescribed consumer actions.

Digital fraud

TransUnion uses intelligence from billions of transactions originating from over 40,000 websites and apps to protect digital transactions. The rate or percentage of suspected digital fraud attempts reflect those which TransUnion customers either denied in real time due to fraudulent indicators or determined were fraudulent after reviewing — compared to all transactions it assessed for fraud. The country and regional analyses examined transactions where the consumer and suspected fraudster was located in a select country and region when conducting a transaction.

Synthetic fraud

TransUnion's synthetic fraud findings were based on an analysis of US consumer credit data from the United States, Territories and Protectorates, and US and overseas military bases. It's sourced from more than 50 years of consumer credit data and contains credit information on approximately 400 million consumers.

About TransUnion TruValidate

TruValidate orchestrates identity, device and behavioral insights to help organizations confidently and securely engage consumers across channels at each stage of the customer journey, helping improve conversions, reduce fraud losses and deliver enhanced, friction-right user experiences.

transunion.com/truvalidate

About TransUnion

About TransUnion TransUnion is a global information and insights company with over 12,000 associates operating in more than 30 countries. We make trust possible by ensuring each person is reliably represented in the marketplace. We do this with a Tru™ picture of each person: an actionable view of consumers, stewarded with care. Through our acquisitions and technology investments we have developed innovative solutions that extend beyond our strong foundation in core credit into areas such as marketing, fraud, risk and advanced analytics. As a result, consumers and businesses can transact with confidence and achieve great things. We call this Information for Good® – and it leads to economic opportunity, great experiences and personal empowerment for millions of people around the world.

transunion.com/business