TransUnion

EBOOK

# Identity Fraud Trends Impacting Government Agencies in 2025

## Reduce fraud, waste and abuse to help improve program efficiency

Government efficiency has recently come into sharp focus, with a particular emphasis on reducing fraud, waste and abuse. Across all levels of government, agencies have worked for decades to enhance constituent services by enabling digital-first customer experiences. As program and benefit administration has become more streamlined via digital channels, constituent preference for completing many administrative tasks in this manner is clearly evident.

However, greater reliance on digital channels to deliver services, such as program and benefit enrollment and administration, has attracted more criminal activity – and none more so than identity-based fraud. TransUnion® analyzed our fraud signal data (device intelligence, data breaches, synthetic identity risk models and identity verification transactions), uncovering trends that reflect elevated levels of fraud risk for the public sector in 2025.

To combat the increased risk and help ensure efficient digital service delivery, government agencies should consider how enhanced risk signals – enabled by a clearer picture of identity – may improve fraud detection and the constituent experience.

## Key takeaways

**6.7%**

of government transactions were suspected digital fraud, a 33% increase from 2023 to 2024

**13.2%**

of government agency identity verification checks had Social Security number (SSN) mismatches

**0.08%**

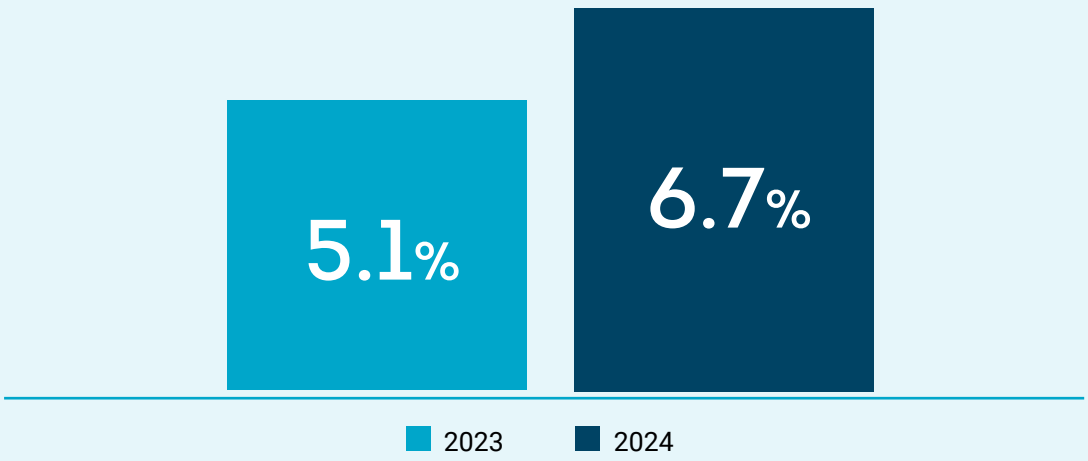
of government digital identity verification checks were suspected of being a synthetic identity

# Fraud trends impacting government agency program efficiency

### Digital transaction fraud risk is rising

The rate of suspected digital fraud among US TransUnion TruValidate™ Public Sector customers was 6.7% in 2024, a 31% increase from 5.1% in 2023. Millions of account login and account creation transactions were flagged for review or denied outright by TruValidate customers due to a combination of risk signals specific to the device being used.

**Public Sector Rate of Suspected Digital Fraud**



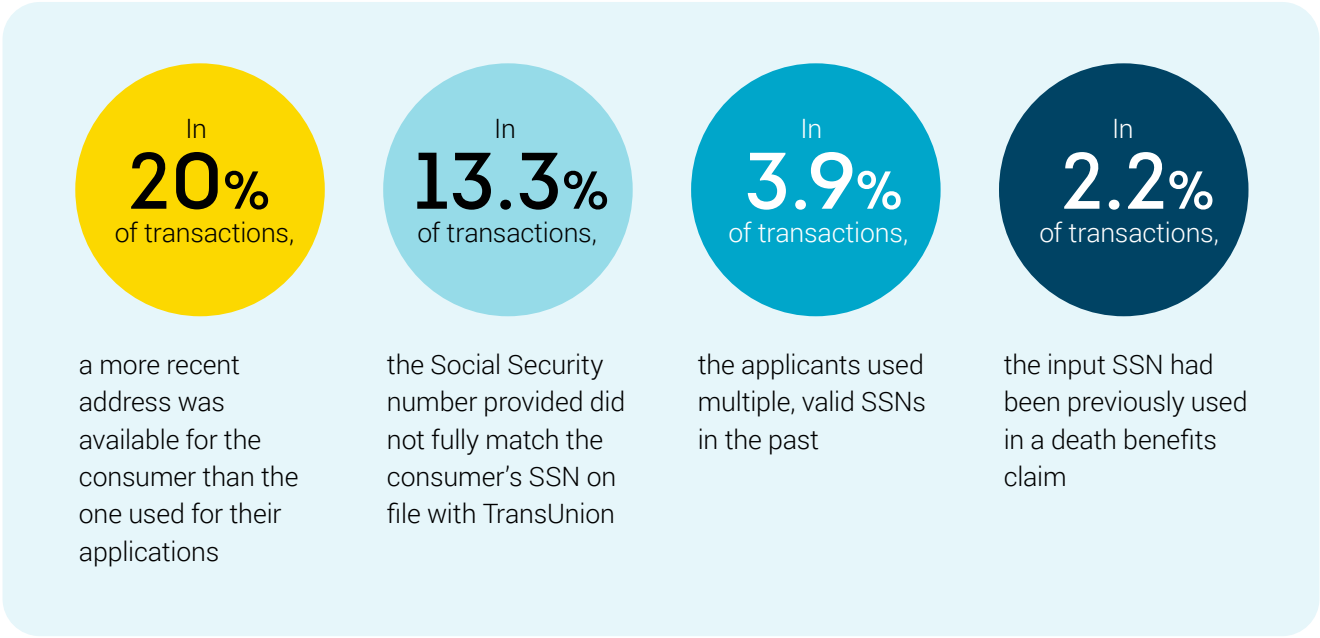

*Source: Internal TransUnion Analysis*

The most common risk signals among suspicious transactions reflect the nature of fraud schemes targeting government programs. They include:

- Using a single device to compromise many different accounts enables fraudsters to operate at scale
- Receiving high transaction volumes from outside the US, including countries like the Seychelles, Kyrgyzstan and Honduras
- Masking a device's location using a virtual private network (VPN) or similar technology to attempt to mask the location of the device

**Identity-based fraud is becoming more widespread**

Basic identity verification checks during benefit enrollment, including SSN and constituent address, are standard methods to combat fraud. Using a random sample of over 550,000 identity verification transactions for consumers enrolling in benefits programs during 2024, TransUnion identified numerous signs of elevated fraud risk facing government agencies:




**Synthetic identity is a hidden government risk**

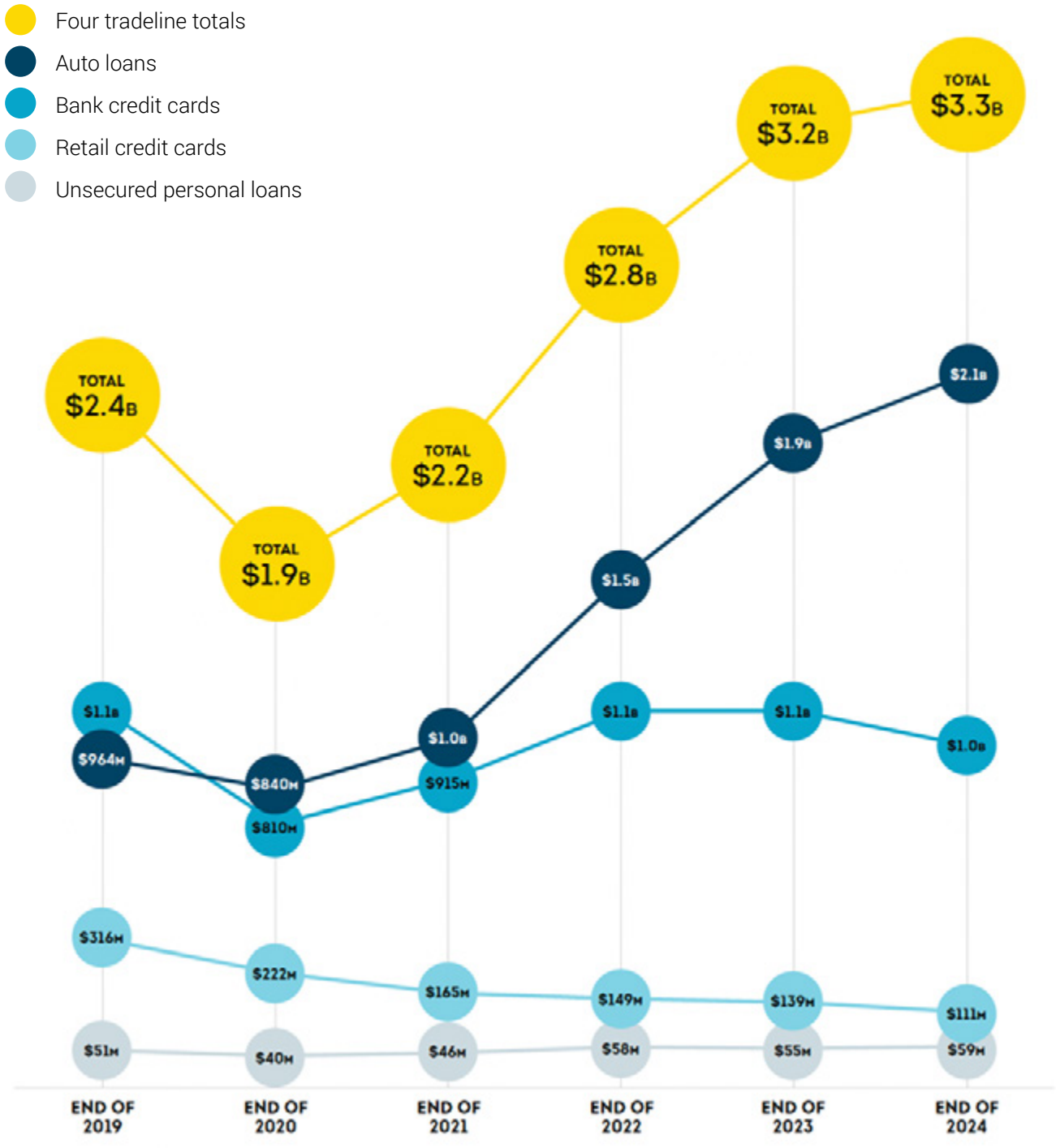
The total exposure to synthetic identities among accounts opened by US lenders for auto loans, bank credit cards, retail credit cards and unsecured personal loans reached USD$3.3 billion in potential losses, an increase of 3% over the end of 2023, according to TransUnion's H1 2025 State of Omnichannel Fraud Report. Government agencies may be exposed to synthetic identity fraud risk but may not know it.

In a review of 550,000 government identity verification transactions in 2024, TransUnion found 0.08% were potential synthetic identities. This may seem insignificant, but these identities could wreak long-term havoc on government programs because they're so difficult to detect.

For example, the most recent IRS statistics (tax year 2022) showed there were 108 million tax returns filed that were issued a refund – with an average amount of $3,280. If 0.08% of those returns (86,400) were submitted by synthetic identities, the IRS could be exposed to $283 million in potential fraud losses for a single year alone.

**Synthetic Identity Risk for US Lenders 2019-2024**

The total credit amount (USD) synthetic identities have access to for US auto loans, bank credit cards, retail credit cards and unsecured personal loans




*Source: TransUnion TruValidate*

# Exposed consumer identity information elevates risk of future fraud

Public sector agencies face elevated risk for both constituents and their organizations as consumers' personal information used in identity proofing is increasingly commoditized via data breach exposures. The severity of data breaches reached record levels, according to TransUnion's H1 2025 State of Omnichannel Fraud Report. The report noted fraudsters are increasingly turning to government programs to monetize stolen identities they purchase. Among reasons for doing so included:

- Perceived weaknesses in digital identity verification and authentication
- Fragmented systems enable a stolen identity to be used to target multiple programs
- Limited ability for victims to see which benefits are being claimed in their names

In 2024, TransUnion TruEmpower™ identified over 2,400 breaches with the potential to enable fraud schemes against government agencies – like tax fraud, document fraud, benefits fraud and identity theft. Collectively, these breaches exposed over 1.6 billion consumer records.

According to TransUnion's Q4 2024 Consumer Pulse Report, 30% of respondents said they'd been recently notified they were among those impacted by a data breach. Consumers frequently respond to these notifications by placing a credit freeze – which can stop financial fraud but will not affect fraudsters targeting government agency programs. Without the means to protect their identities from being misused, constituents rely on agencies to protect them from identity-based fraud.

**1.6 billion consumer records exposed by data breaches in 2024 – with the potential to enable government fraud, waste and abuse, including:**

**585 million** Social Security numbers

**529 million** driver's license numbers

**121 million** US passport numbers

*Source: TransUnion TruEmpower*

# Agency digital-first customer experiences increase risk exposure

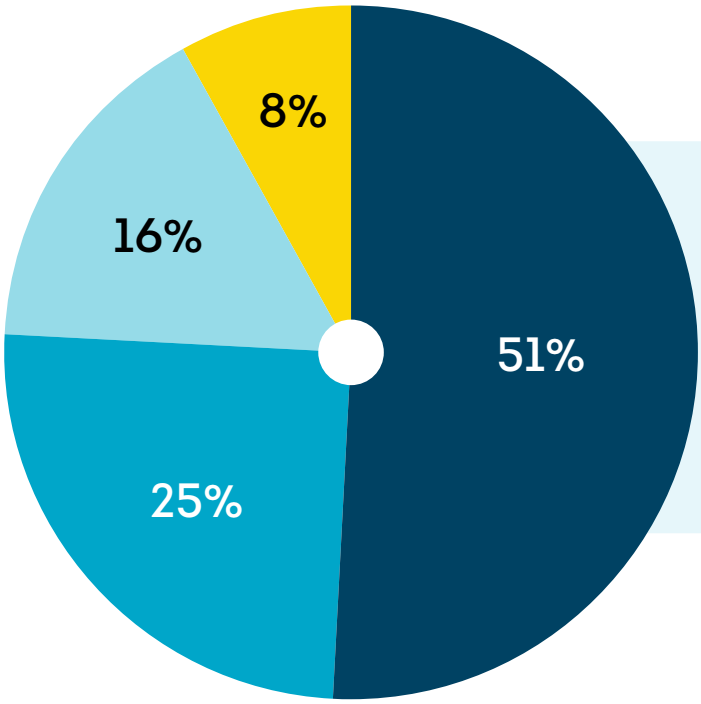
Government agencies have focused on improving agency program efficiency by implementing digital-first, omnichannel customer experiences for decades. This has benefited constituents and agencies alike, and a recent consumer survey found most constituents start their enrollment processes online and prefer email for ongoing program notifications.

However, recent trends in omnichannel fraud point to increased risk for government agencies' digital-first, customer experience strategies. Half (52%) of Americans reported being targeted with email, online, phone call or text message fraud scheme from August to December 2024, according to TransUnion's H1 2025 State of Omnichannel Fraud Report. In addition, 6% of calls into US call centers in 2024 were identified as having a high risk for fraud.

Criminals increasingly exploit digital channels to perpetrate fraud, putting more government programs at risk. Harnessing vast stores of exposed identities from data breaches and consumer scams, combined with AI enabled technology, fraudsters can attack agencies and constituents at will. Despite the risks, constituent preference for using convenient digital channels to interact with government agencies demands greater focus on reducing fraud, waste and abuse at the point of service.

**Online application preferred for program enrollment**

Preferred channel for program enrollment.



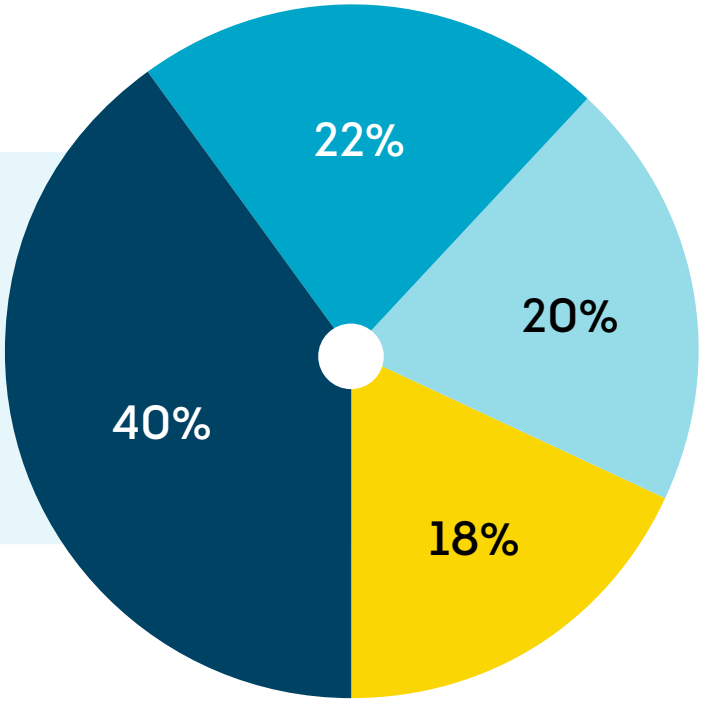

- Filling out an online application
- In-person at the nearest office
- A phone call with an agency representive
- Mailing in an application

*Source: TransUnion consumer survey 2024*

**Email is preferred communication channel for program notifications**

- Email me
- Text Me
- Call Me
- Send me a letter in the mail

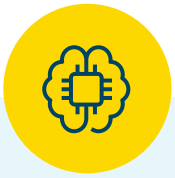
*Source: TransUnion consumer survey 2024*



# Enhance fraud detection with a clearer view of identity

Now is the time for government agencies to review their fraud detection measures to help ensure they stack up against the ever-changing reality of how fraud is perpetrated. Criminals emboldened by enormous quantities of exposed consumer identities – in addition to new technologies at their disposal – are developing increasingly sophisticated and hard-to-detect schemes that will challenge agencies that haven't kept up with the pace of change.

**Four fraud detection questions that must be answered to help protect government programs from fraud, waste and abuse:**



### Can you detect AI-generated images of official documents?

The markers of generated images are different from those in manipulated images — possibly evading legacy document authentication detection technologies.

### Can you identify spoofed calls into your call centers?

Fraudsters can use stolen identities and phone numbers in conjunction with non-fixed VOIP technologies to convincingly impersonate their victims when engaging call center agents.

### Can you spot synthetic identities that apply for programs or benefits?

The use of real identifying information to create a fake beneficiary is difficult to detect and requires the use of signals beyond what's included on a program or benefit application.

### Can you flag suspicious devices used in remote transactions?

Incorporating device-level intelligence alongside identity information can help reduce fraud by flagging devices with risk indicators — such as a recent SIM card swap, geolocation mismatch or device being used for an identity it has never previously been associated with.

## Actionable steps to help improve public sector efficiency and constituent experiences

As agencies look to bolster omnichannel constituent experiences, fraud protection can help boost constituent trust – and help reduce fraud, waste and abuse. But discerning fraud risk requires the right controls to maintain efficient verification, authentication and enrollment.

Differentiating between legitimate constituents and bad actors can get more complicated as agencies use more channels. However, with enhanced risk signals – including device-to-identity linkages – agencies can more successfully authenticate a user's identity in their preferred channel. They can also apply step-up challenges more intelligently without burdening legitimate constituents and optimize operational costs by reducing false positive reviews.

**It's time to engage constituents with a clear picture of identity**

Learn how TransUnion fraud solutions – powered by our identity data network – fuels AI, enabling more precise fraud detection, fewer false positives and stronger protection at every touchpoint.

**Visit transunion.com/public-sector to learn more.**



TransUnion