Improper payments in the public sector

Improper and unknown payments continue to contribute to financial waste in government spending.

$214B+ in improper payments made in FY 2022

41% increase in improper and unknown payments from 2019 to 2022

To build trust and credibility with the communities they serve, the public sector needs to manage the financial and reputational risk, while improving the user experience from end to end.

Use emerging technology that can learn and correct discrepancies via return intelligence

Interrogate multiple data sources for optimized results

Have confidence in validation and authentication with identity proofing processes

Employ frictions, straight-through processing

Addressing improper payments

As little as three steps to improvements in addressing improper payments.

1. Build a technology framework
Better technology can help reduce the need for manual processing, improve payment times and lower the error rate.

2. Leverage data to prevent fraud
Use data analytics to increase accuracy, proactively prevent errors and mitigate payment fraud.

3. Improve the user experience
Enhance all aspects of the payment experience, including identity validation and payment account verification, to minimize improper payments.

Defend against fraud
Take action to help protect against fraud and improper payments.

Validate recipient accounts
- Mitigate risk of payments fraud as technology advances
- Reduce identity takeover and re-direction of funds to unauthorized recipients
- Manage operational, collection and recovery costs from payments fraud more effectively
- Minimize reputational risk, which can be just as damaging as financial losses

AVS use cases
Account Validation Services helps government entities and GSEs overcome challenges.

1. Help ensure payment accuracy
   - Low return/cancellation rates
   - Ensure funds are sent to the right recipient
   - Reduce risk of identity theft
   - Minimize late payments

2. Work to prevent identity theft
   - Simplify tax payments and earned income credits
   - Validate the account owner and the disbursement details
   - Mitigate risk associated with processing a refund

3. Protect constituent data
   - To make changing bank details more secure
   - Authenticate and validate account information
   - Reduce vendor financial information before updating details

4. Issue emergency payments and benefits
   - For tax due and recurring payments, ensure providers provide the correct recipient information
   - Mitigate the account system’s risk, ownership and associated risk

Sources: