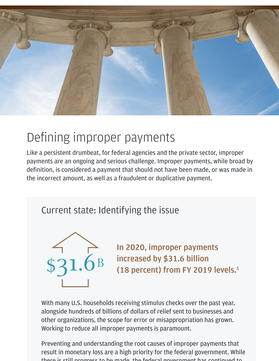
Addressing improper payments: strategies for the public sector

The rise in misappropriated funds has prompted a shift in how industries in both the public and private sectors address the prevention and reduction of improper payments—aiding in successfully introducing new data mechanisms and improving user experience.

BY: **EVA ROBINSON**, INDUSTRY HEAD FOR GOVERNMENT AND PUBLIC SECTOR, J.P. MORGAN PAYMENTS.
STEVE BERNSTEIN, N.A., PAYABLES PRODUCT SOLUTIONS, J.P. MORGAN PAYMENTS



Defining improper payments

Like a persistent drumbeat, for federal agencies and the private sector, improper payments are an ongoing and serious challenge. Improper payments, while broad by definition, is considered a payment that should not have been made, or was made in the incorrect amount, as well as a fraudulent or duplicative payment.

Current state: Identifying the issue

$31.6 B

In 2020, improper payments increased by $31.6 billion (18 percent) from FY 2019 levels.[1]

With many U.S. households receiving stimulus checks over the past year, alongside hundreds of billions of dollars of relief sent to businesses and other organizations, the scope for error or misappropriation has grown. Working to reduce all improper payments is paramount.

Preventing and understanding the root causes of improper payments that result in monetary loss are a high priority for the federal government. While there is still progress to be made, the federal government has continued to make substantial strides towards enhancing efforts in identifying methods for the detection, prevention and recovery of improper payments.

Examining improper payments has created an opportunity to develop counter-acting tools to address the issue, and has opened the door for public and private exchange of information, experiences and learnings.

Taxpayers expect efficiency and minimized wastage, and ensuring taxpayer dollars are properly allocated is a critical function of the federal government—which has caused improper payments to become an elevated concern.

Improper payments negatively impact profitability. This friction leads to losses within the private sector, and can result in higher taxes and wasteful spending in the public sector. Although not all improper payments are a result of fraud, they all have the potential to erode trust and question why more is not being done.

Reshaping strategies for prevention and reduction of improper payments

Here are three primary conditions that are contributing to improvements in addressing improper payments in the public and private sector.

1. Executing a successful onboarding experience is essential

The benefits of reducing improper payments are significant. The most obvious is the hard dollar savings that can be delivered preventively. As a result of ongoing issues, the federal government has the opportunity to leverage best practices and advanced solutions from the private sector to augment its payment systems.

Commercial solutions that focus on identity and bank account validations are helping corporations and government agencies in managing improper payments by providing access to state-of-the-art fraud detection and prevention tools. Fraud mitigation and preventative tool utilization have become a necessity for enabling the validation and authentication of individual payments to root out improper or fraudulent payments prior to release of funds.

Building the framework for addressing improper payments

There are several important pivot-points that can create the framework to address improper or fraudulent payments:

Through use of tools, straight-through processing results can improve markedly, reducing the need for manual processing and customer interaction. This also allows federal agencies and other payors to redirect their resources towards exceptions and complex cases, which can help in improving both payment times and lowering the error rate.

Two examples are tools that can:

Verify bank account data in order to ensure an error-free follow-on payment.

Authenticate the identity of the counterparty consumer or commercial entity by cross-referencing a number of data elements—address, name, national ID, for example.

Increasing automation in payments processing is also vital, as it adds capacity. Manual processing is both time-consuming and can result in errors, especially when there is a large increase in applications for programs, such as benefits or tax refunds.

Authenticating the identity of a beneficiary as well as validating "credentials" across multiple government agencies makes it possible to get a "single source of truth" for each individual or business. This enables agencies to verify that payments are not being sent twice, or that individuals are only receiving payments they are entitled to.

Improper payments FY 2018–2020

	Improper payment (in USD)[1]	Improper payment rate[1]
FY 2020	$206 B	5.6 %
FY 2019	$175 B	5.1 %
FY 2018	$151 B	4.6 %

2. Mitigating improper payments with AI and data

Financial institutions have integrated emerging technology and innovative solutions to maximize payment efficiency, which can greatly reduce improper payments within the public and private sector. For example, deploying the latest data analytics and machine-learning techniques can increase accuracy, allowing agencies to scale processing volumes with minimal exceptions. Previously, some data analytic approaches sought to detect errors after improper payments had been made —creating a time-consuming and expensive resource in attempting to recover funds or correct data.

Utilizing emerging technologies that are designed for detection, such as "pre-listing", an existing attribute, can proactively prevent errors and mitigate payment fraud. For example, analyzing an account's transaction history, when an account was opened, identifying associations, and counterparties and payment history can provide an indicator of whether the payment should be stopped, reviewed or commence.

Enabling artificial intelligence (AI) by applying real-time correction based upon sourced proprietary or accessible databases, can be effective in improving automation. These solutions are able to identify if a piece of information—such as an address or account routing number—is incorrect, and automatically correct it. The information is then fed back into the system so that over time the AI algorithm becomes more accurate.

3. Improving the user experience with multiple-data pools

A key element of addressing improper payments is the ability to grow machine-learning attributes through ongoing data and payment handling, while continually improving the sophistication of its analytic tools. Today, users may be required to validate their identity multiple times across various government agencies, or payments can be delayed due to missing information. Utilizing multiple data analytics tools can enhance all aspects of the payment process, while prioritizing prevention and recovery for improper payments.

As shown below, business e-mail compromise (BEC) has also contributed to fraudulent and improper payments. As we conduct more of our business and financial lives online, bad actors continually seek to exploit consumers and businesses when they are most vulnerable to e-mail compromises, an important use case for account validation prior to payment storage and processing.

Payment fraud trends—BEC fraud leads

Sources of attempted and/or actual payments fraud in 2020[2]

Business email compromise	62 %
Outside individual	52 %
Third-party or outsourcer	19 %
Account takeover	12 %

Payments methods impacted by business email compromise in 2020[2]

Wire transfers	43 %
ACH credits	34 %
ACH debits	16 %
Checks	14 %
Corporate credit cards	9 %
Gift cards	2 %

Leveraging blockchain networks

Blockchain technology—a secure and encrypted digital database shared by all parties in a distributed network—is another technology area that has great potential for reducing improper payments. All transactions occurring within the network are recorded, verified and stored in a database that is accessible to all participants through an unalterable transaction tracker. A peer-to-peer blockchain network that allows banks and other financial services organizations to share payment information with each other are commercially available today. These networks can also enable organizations to pre-validate account information in near real time, before a transaction is made. Importantly, adopting preventative solutions and techniques, can help agencies comply with regulatory and statutory payment requirements without resorting to a "pay and chase" approach.

Key strategies

1. Adopting a strong onboarding process, while enforcing industry best practices and advanced technology has the potential to significantly cut improper payments with minimal exposure for the tax payer.
2. Implementing automation, big-data analytics and machine learning like AI into payments systems can greatly reduce the rate of error for financial institutions.
3. Adopting blockchain technology in order to connect participating network partners—which updates and re-uses validated data points crucial to successfully executing payments, while mitigating risk.

Public-private partnerships and information exchanges have proven successful in addressing challenges with payments and a means of sharing best practices. The opportunity to establish standards and conduct co-creation exercises has become more prevalent and relevant as the issue of improper payments continues to challenge agencies.

Connect with your J.P. Morgan representative to learn more.

[1] "Annual improper payments datasets," paymentaccuracy.gov. Available at: https://www.paymentaccuracy.gov/payment-accuracy-the-numbers/

[2] 2021 AFP Payments Fraud and Control Survey Report

J.P.Morgan