



February 27, 2023

Preventing Improper Payments: Lessons from Using Data Matching in Pandemic Relief Program Oversight

For the past several decades, data matching has enabled the use of government data to identify fraud, waste, abuse, and mismanagement in benefit programs. Data matching is the comparison of different datasets to identify similarities in the records each dataset contains. Matches can be made using one or more data elements, such as name, address, email, bank account number, internet protocol address, or Social Security number (SSN).

Oversight of federal funding for pandemic relief programs is a recent demonstration of how data matching can be used to detect improper payments. An improper payment is a payment that should not have been made, either in its entirety or in the wrong amount.

The Pandemic Response Accountability Committee (PRAC) was established by the Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136) as part of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The PRAC is responsible for providing transparency and oversight of pandemic programs and expenditures. Since 2020, oversight agencies, including the PRAC, have identified tens of billions of dollars of COVID relief funding that may have been compromised by potential fraud, waste, or abuse.

One way the PRAC has worked to detect improper payments is through data matching using a “data platform” it developed. The chair of the PRAC testified that this data platform gives the PRAC access to more than 150 million records to detect improper payments across a number of pandemic relief programs.

This In Focus discusses the data platform established by the PRAC, the risk of improper payments in pandemic programs, and how, according to the PRAC and agency inspectors general (IGs), data matching can be used to prevent improper payments. There are several issues Congress might consider on the use of data matching in detecting and preventing improper payments.

Pandemic Analytics Center of Excellence

The PRAC has the statutory authority to conduct and support oversight of all pandemic spending across executive agencies. To support this role, the CARES Act extended to the PRAC the authority given to IGs, including to access agency records and request information to carry out its responsibilities (134 Stat. 537; 5 U.S.C. App. §6).

In August 2021, the PRAC established the Pandemic Analytics Center of Excellence (PACE), a data platform managed by the PRAC’s chief data officer in coordination with the chief information officer. CIGIE has issued several

contracts to support PACE’s technology and data infrastructure and its various analytic capabilities.

PACE’s operation broadly enables data sharing and data analytics across IGs and law enforcement and assists in investigations and audits of pandemic relief programs. PACE is used to conduct data analysis, including data matching and network analysis, and to develop data services, including natural language processing and risk modeling. PACE supports the investigative work of IGs and the PRAC Fraud Task Force by uncovering potential fraud and investigating leads.

For instance, PACE matched Economic Injury Disaster Loan (EIDL) and Paycheck Protection Program (PPP) data from the Small Business Administration (SBA) to create fraud risk scores for both individuals and specific applications. PACE has also developed a model for the Department of the Treasury to score the risk associated with 79,000 prime and subrecipient awards to state and local governments under the Coronavirus Relief Fund (CRF). Treasury has used these scores to focus its reviews on higher-risk CRF awards.

A “Data Platform” for Oversight Is Not New. PACE is modeled after practices developed by the Recovery Accountability and Transparency Board’s Recovery Operations Center (ROC), which supported oversight of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5). ROC demonstrated that the government could better detect improper payments through data matching.

A report from the Government Accountability Office stated that preservation of ROC’s capabilities could help sustain oversight of federal expenditures in general. Although Congress authorized Treasury to take over ROC, it was dissolved in 2015, effectively terminating the capacity and expertise developed by ROC. While the PRAC is scheduled to sunset in 2025, PACE could become a long-term data platform for the IG community.

Risk of Improper Payments in Pandemic Programs

Congress provided over \$5 trillion for the response to the COVID-19 pandemic and its consequences. The amount of funding appropriated, the scope and complexity of key relief programs, and the focus on rapid disbursement of funds to businesses and individuals all contributed to the risk of improper payments for pandemic programs.

Another risk factor for improper payments in some pandemic relief programs, such as the Pandemic Unemployment Assistance (PUA) program, was the role of states in their administration. According to the IG

community, some states were better prepared than others to implement pandemic programs with the appropriate controls given the focus on rapid disbursement. States also depended on guidance from the administering federal agency to implement program operations and related processes. Some observers have stated that such guidance may have been unclear or insufficient, making it difficult for states to ensure program integrity.

It appears that there were some opportunities for individuals and groups to intentionally defraud programs and take advantage of the circumstances of relief program administration. One such opportunity was self-certification of eligibility that required no verification or validation. It has been suggested that given the scale of the programs, investigators will likely be identifying and pursuing pandemic program fraud for years to come.

Lesson Learned: Using Data Matching to Prevent Improper Payments

The PRAC published *Lessons Learned in Oversight of Pandemic Relief Funds* in June 2022 that details 10 “lessons learned” from its oversight of pandemic relief programs. Several of these lessons suggest data matching can be a tool for both detecting and *preventing* improper payments. Specifically, the PRAC has asserted that:

- data matching with existing data should be used in program administration to support determinations of eligibility and to identify potential fraud, and
- validating information using data matching could reduce the possibility of fraud and risk of improper payments.

That is, in PRAC’s view, had data matching been used for such purposes to administer pandemic relief programs from the beginning, the risk of improper payments in pandemic relief programs might have been mitigated.

Vast amounts of data already exist, which can be used in data matching to prevent improper payments. These existing data may be sourced from databases maintained by federal agencies or state governments or from private, nonprofit, or commercial providers. These data could be matched with information supplied on an application to verify the information and determine the eligibility of an applicant for a benefit program. Examples include matching to validate SSNs, matching to prison records to detect potential fraud, and matching to records in Treasury’s Do Not Pay (DNP) system to verify an individual’s eligibility for federal benefit payments.

In February 2023, for example, the PRAC issued a “fraud alert” involving SSNs that were not sufficiently verified by the SBA using Social Security Administration (SSA) data. PACE identified \$5.4 billion in potentially fraudulent PPP and EIDL loan applications that used questionable SSNs by matching such loan applications with SSA data. The PRAC stated that the SBA should have been required to access to SSA data to verify the accuracy of SSNs used on PPP and EIDL applications.

Similarly, the Department of Labor (DOL) IG has reported that matching data of unemployment insurance applicants with existing databases on individuals in state and federal prisons could act as one fraud control mechanism. Incarcerated individuals may be ineligible for these programs or the targets of identity thieves submitting fraudulent claims. The DOL IG estimates that up to \$98.3 million in CARES Act funding in 2020 for PUA was fraudulently paid on applications that used incarcerated individuals’ information.

Another source of existing data is the DNP system, which is governed by the Payment Integrity Information Act of 2019 (P.L. 116-35), which Congress passed to improve government-wide payment integrity by requiring agencies to review available databases with information on eligibility before releasing funds. It ensured agency access to the DNP system as one of those databases. The SBA IG used the DNP system retrospectively, matching data of EIDL recipients with records in DNP, and found that \$3.65 billion was distributed to potentially ineligible recipients between March and November 2020. SBA did not originally use the DNP system to mitigate the risk of improper payments.

Issues for Congress

Congress has empowered the PRAC to address improper payments and to access and use data to carry out its oversight of pandemic relief programs. Congress may consider whether to extend the PRAC data platform’s capabilities beyond pandemic programs for the IG community.

Congress might consider how the benefits of operating a data platform compare to its direct and intangible costs, including risks to privacy and the security of the platform. This could include congressional oversight of how IGs are using the data platform that is enabled by their relatively broad access to agency data. Congress regulates how agencies use the data they collect on individuals but has been more open to IGs using data matching and may create guardrails as IGs do more with their authority.

The work of the PRAC may also provide Congress a springboard to explore more closely agencies’ data capabilities to *prevent* improper payments. The Computer Matching and Privacy Protection Act (P.L. 100-503) establishes the requirements and processes by which executive agencies may use data matching to administer benefit programs (see CRS Report R47325, *Computer Matching and Privacy Protection Act: Data Integration and Individual Rights*, by Natalie R. Ortiz). To try to minimize improper payments in benefit programs, Congress might examine how it can best facilitate data matching and examine whether current statutory mechanisms effectively enable data matching in the way and on the scale it desires.

Natalie R. Ortiz, Analyst in Government Organization and Management

Ben Wilhelm, Analyst in Government Organization and Management

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.