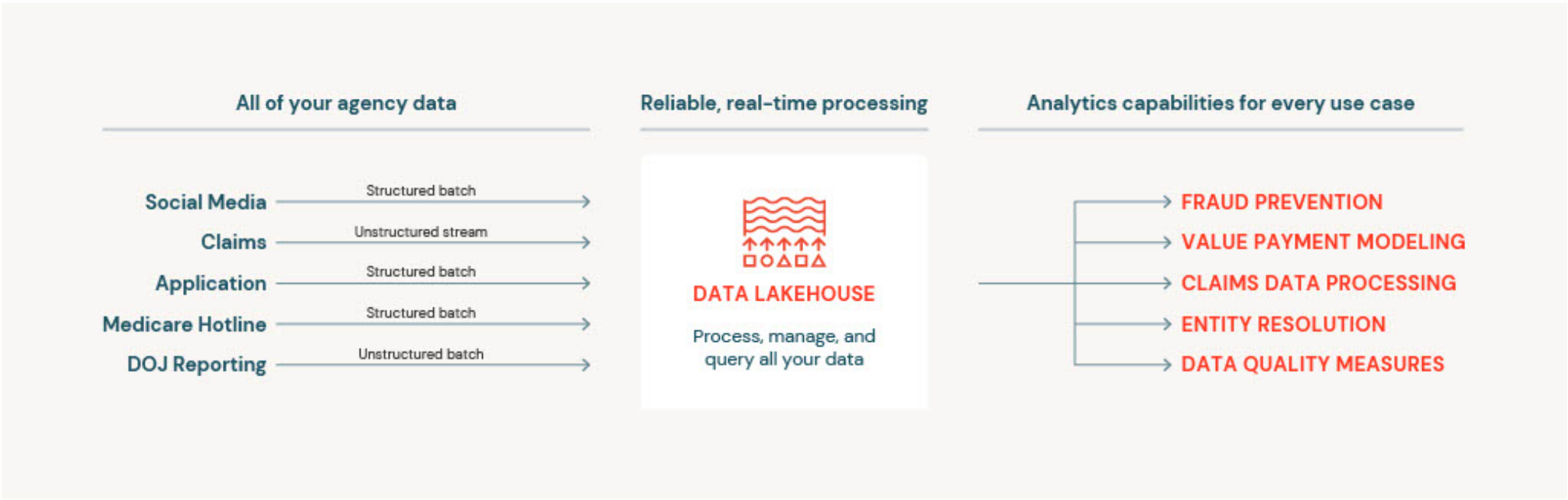
Leveraging Databricks to Prevent Improper Payments

With Databricks Lakehouse for Public Sector, it's finally possible to combine all of an agency's data — whether structured, unstructured or semi-structured — in a centralized platform and analyze it in a fast, cost-effective way. Agencies can tackle enormous problems like FWA with advanced analytics, making it possible to gain a complete picture of the citizen, detect unusual application patterns and ascertain their correlation to potentially fraudulent activity, or identify administrative or application errors.



The Data Solution: From Pay-and-Chase to Proactive Prevention

Fortunately, government agencies know data provides a way forward. The CMS Center for Program Integrity has stated that in their efforts to protect taxpayer dollars and "enhance and modernize program integrity to combat fraud, waste, and abuse" they are working to:

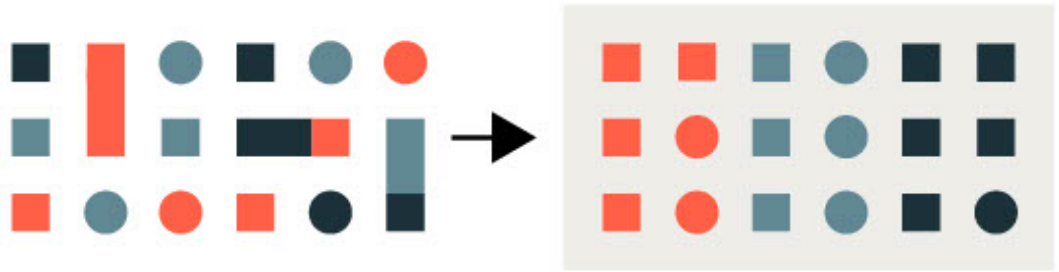
- Leverage new and emerging technology to modernize program integrity tools
- Protect enrolled providers while taking aggressive actions to keep out those who seek to defraud the programs
- Use data to identify and address key risk drivers to mitigate emerging Medicaid eligibility program risks
- Target services and supplies at high risk for Medicare fraud for additional review, while reducing provider burden

A modern data solution gives agencies the tools to break down data silos, bringing all data into a central lakehouse where data is curated from raw to refined, to ready-for-analytics. This curation activity addresses data quality challenges, while identity resolution creates a more complete picture of the citizen or entity.

Leveraging the power of AI and ML, a data lakehouse can empower agencies to detect suspicious activity or application errors before a payment is issued, rather than chasing reimbursements after the fact. In fraud detection, AI "can spot abnormalities and outliers that can be referred to human investigators to determine if fraud actually has taken place," according to researchers at the Brookings Institute.

Such an approach can help agencies evolve from the "pay-and-chase" model to a more predictive and preventative footing.

Break down data silos, transform, organize and leverage data of all types for analytics use cases.



Negative Impacts of Doing Nothing

With improper payment statistics trending upwards in recent years, status quo pay-and-chase efforts have proven to recover only a fraction of improper payments. But the impact goes beyond monetary, as inadequate mitigation erodes trust in the government's management of important entitlement programs.

Continued loss

Fraudsters aren't going away any time soon. But, it's estimated that only one-third of improper payments are due to deliberate fraud. Not taking a proactive approach means agencies are also missing opportunities to prevent application errors and administrative oversights that result in improper payments.

Eroding confidence

With skepticism about the government already high, agencies cannot afford a rate of FWA that will only continue to undermine confidence in program oversight.

Increased scrutiny

For state agencies, lack of payment integrity may result in scrutiny from CMS, including "an organization-wide audit of the Medicaid program," according to the HHS Comprehensive Medicaid Integrity Plan.

Today's data architectures make it possible for agencies to break down silos and centralize program data in a single location. Modern solutions support identity resolution for a complete picture of the citizen and can leverage advanced analytics, AI and machine learning to provide agencies with proactive tools in the fight against FWA.

The Current State of Loss and Recovery Mitigation

In the battle against improper payments, government agencies have taken a mostly reactionary approach to recover erroneous payments and are burdened by structural challenges. These include:

Pay-and-chase

In "pay-and-chase," programs make payments with little scrutiny, and then when discrepancies are noticed at a later date — caused either by intentional fraud or human error — they try to recoup those funds. This puts an undue burden on taxpayers, who must bear the cost of the error, and then the expense of the chase. And it's ineffective, often failing to redress the loss.

> "For too many years, we have played an expensive and inefficient game of 'whack-a-mole' with criminals — going after them one at a time — as they steal from our programs."
>
> Former CMS Administrator Seema Verma

The human element

Driven in part by the pay-and-chase model and general limitations on resources, most agencies find they have a backlog of FWA investigations, with fraud investigators often understaffed and overwhelmed.

The human element is significant, especially when agencies take a manual investigation approach to FWA prevention and remediation. If staff is stretched too thin, as is often the case, agencies will struggle to keep up with the sheer volume of cases and improper payments will go either unnoticed or unchecked.

Outdated IT

Antiquated data architecture further complicates the picture. Agencies may be hampered by data silos, inadequate data management capabilities or data science expertise, preventing the detection of improper payments before checks are cut and sent out the door.

How the Covid Pandemic Accelerated Fraud

As the COVID pandemic ushered in an easing of government oversight and the deployment of $5 trillion in relief funds for struggling Americans, small businesses and healthcare providers, the stage was set to unleash rampant fraud.

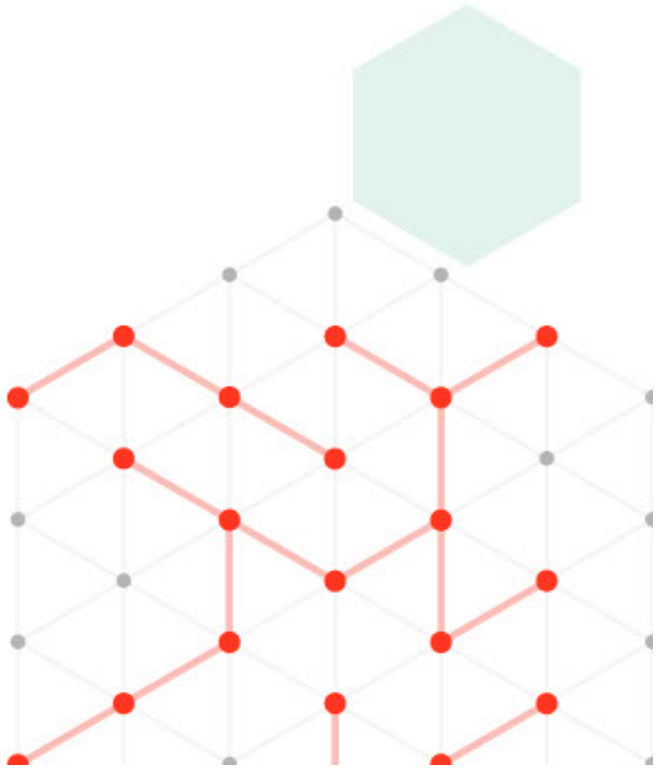
> "The Small Business Administration, in sending that money out, basically said to people, apply and sign and tell us that you're really entitled to the money. And of course, for fraudsters, that's an invitation."
>
> Michael E. Horowitz, Chair, Pandemic Response Accountability Committee, Inspector General, U.S. Department of Justice

According to NBC News reporting:

- One fraud ring stole $20 million by using fake IDs to apply for loans for fake businesses
- One building in San Francisco was listed on 1,300 different pandemic relief loan applications
- NBC reported that billions in pandemic relief funds have been lost to fraud

> "What didn't happen was even minimal checks to see if the money was getting to the right people."
>
> Michael E. Horowitz, Chair, Pandemic Response Accountability Committee, Inspector General, U.S. Department of Justice

And USA Today reported on how telehealth fraud alone cost Medicare $128 million in the first year of the COVID pandemic.



databricks

Improper Payments by the Numbers

$2.2T since 2003

The U.S. Government Accountability Office (GAO) estimates that cumulative federal improper payments have totaled approximately $2.2 trillion since FY 2003.

$281B in 2021

Federal agencies made an estimated $281 billion in improper payments in FY 2021, up from about $206 billion for FY 2020, according to the GAO.

21.6%

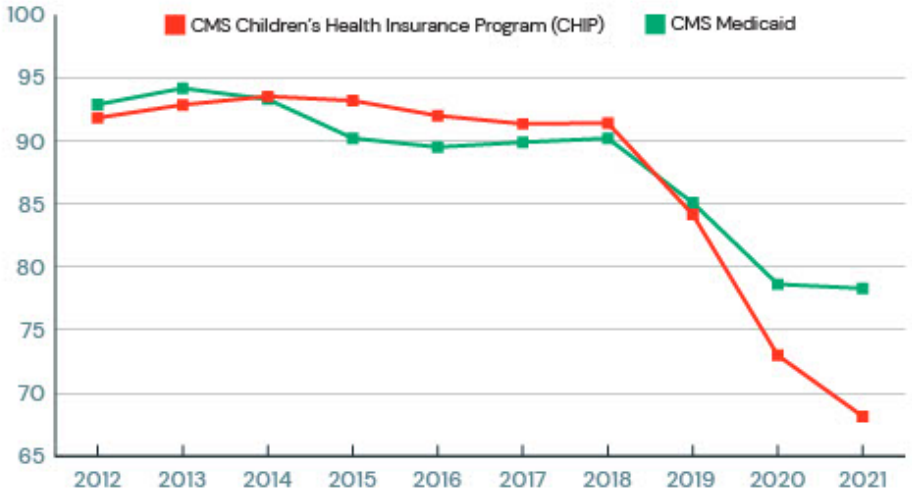
Overall, the CMS Payment Error Rate Measurement program reports the payment error rate in the Medicaid and CHIP programs escalated dramatically in the past decade, from 7.1% in 2012 to over 21.6% in 2021.

$134B

In 2021, total improper payments under Medicare FFS, Medicaid and CHIP topped $129 billion.

23% drop in accuracy

The Children's Health Insurance Program (CHIP), run by the U.S. Centers for Medicare & Medicaid Services (CMS), says payment accuracy dropped from 91.84% in 2012 to 68.16% in 2021, resulting in $5.3 billion in improper payments in 2021 alone.



Introduction

Federal, state and local government agencies exist to serve the public good through entitlement and benefit programs that improve the health, safety and well-being of their constituents. These vital programs, such as Medicare-Medicaid, Supplemental Nutrition Assistance Program (SNAP), and the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC), provide essential health and nutrition entitlements for a vast number of Americans.

Funded with public money, the agencies that manage these programs have a fiduciary responsibility to maintain public trust by ensuring program integrity and effectiveness as they serve the needs of citizens.

But public benefits programs are routinely subject to fraud, waste and abuse (FWA) due to intentional fraud or human error. Improper payments (payments that should not have been made or were made in the incorrect amount) may be issued as a result of errors in claims processing or malicious actors, who, for instance, look for ways to game the system while draining the taxpayer of billions of dollars.

The vulnerability of these programs may be further exacerbated by public health emergency events like the COVID pandemic, or by natural disasters. When government agencies loosen restrictions and move rapidly to deploy assistance, errors and abuse can occur.

Without public trust, government entitlement programs risk eroding taxpayer support and may set themselves up for legislative challenges, cutbacks or defunding.

Fortunately, mitigating FWA and the issuance of improper payments is a problem solvable through modern data management. With a cloud-native platform, agencies can improve program integrity by breaking down data silos and accessing all of their data. Agencies will be empowered to leverage advanced analytics to identify anomalous patterns, errors in applications and duplication, putting the brakes on improper payments before the funds are dispersed.

Contents

databricks

About Databricks

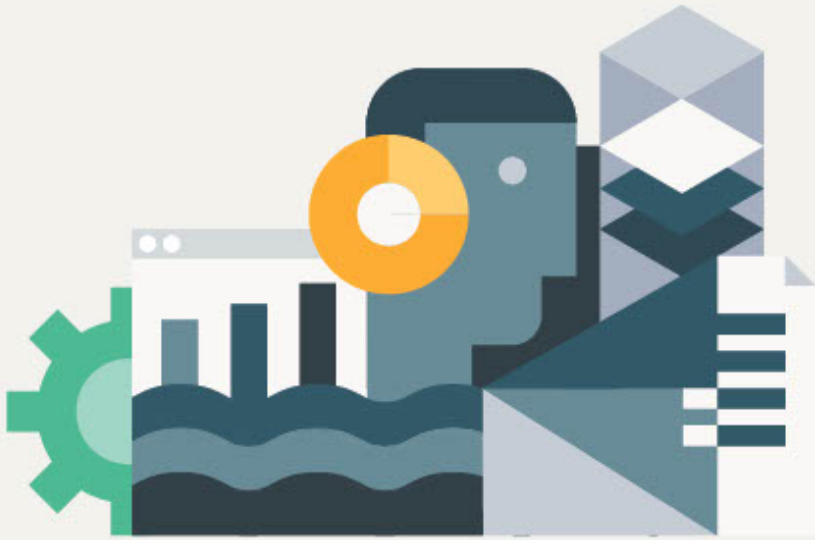
Databricks is the data and AI company. More than 7,000 organizations worldwide — including Comcast, Condé Nast, H&M and over 40% of the Fortune 500 — rely on the Databricks Lakehouse Platform to unify their data, analytics and AI. Databricks is headquartered in San Francisco, with offices around the globe. Founded by the original creators of Apache Spark,™ Delta Lake and MLflow, Databricks is on a mission to help data teams solve the world's toughest problems. To learn more, follow Databricks on Twitter, LinkedIn and Facebook.

Get started with a free trial of Databricks and start building data applications today

START YOUR FREE TRIAL

To learn more, visit us at:

databricks.com/state-local-government



databricks

A Solvable Data Problem With Databricks Lakehouse

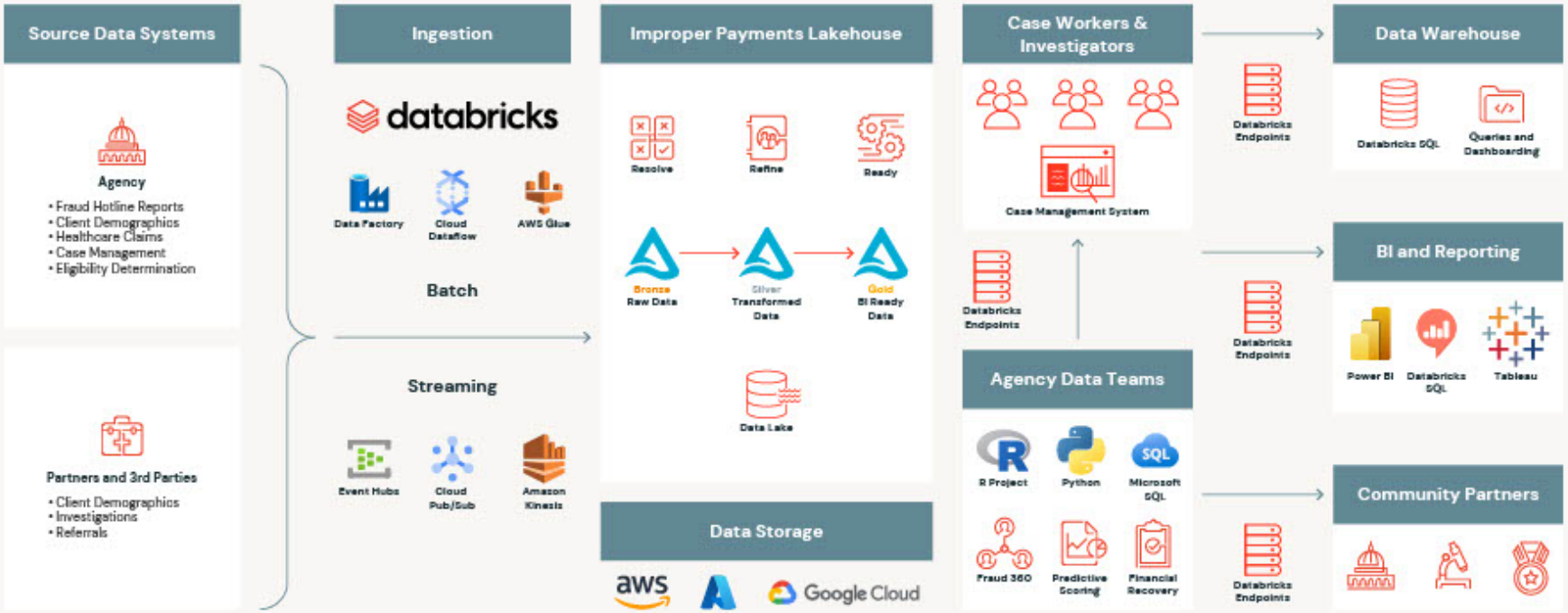
Delivering entitlements to the neediest and most vulnerable is a vital aspect of the services provided by state and local government agencies. But improper payments due to outright fraud on the one hand, and human error on the other, have already cost the U.S. taxpayer in excess of $2 trillion over the last two decades, putting these essential programs at risk.

Reducing improper payments is a data problem best solved with a modern data platform. The Databricks Lakehouse for Public Sector is a cloud-native platform that is easy to set up, manage and scale. Agencies gain the ability to unify data, analytics and AI workloads to automate claims processing, detect anomalies and make predictive decisions while giving fraud investigators access to deeper, more meaningful insights. Databricks Lakehouse gives state and local agencies a modern data advantage in the fight against fraud, waste and abuse.

To learn more about how we are helping the public sector securely leverage data and AI, please visit us at dbricks.co/federal.

databricks

Databricks Lakehouse reference architecture



Fraud, Waste and Abuse Use Cases

With Databricks, agencies can move from a loss recovery model (pay-and-chase) to a more effective preventative control paradigm, which means early detection of improper payments before funds are disbursed.

Consider these use cases:

Data Curation/ETL

Moving toward a more proactive fraud prevention approach requires curation of the various data sources that will be leveraged in detecting improper payments. Databricks Delta Live Tables (DLT) makes it easy to build and manage reliable data pipelines that deliver high-quality data on Delta Lake. DLT helps data engineering teams simplify extract, transform and load (ETL) development and management with declarative pipeline development, automatic data testing, and deep visibility for monitoring and recovery.

The focus should be on curating the most valuable data sets, which may contain highly structured data such as personal or business demographics as well as more semi-structured or unstructured sources such as social networks from social media sites. These various data formats may be ingested in regular batches or even real-time streams.

As these data are ingested, start by establishing a landing zone where source data is kept in its original form. From this raw landing zone, perform data quality and enrichment steps, which transform source data into a more refined set of data.

The final step in curation will be to create a gold layer of data that is ready for analytics. This fine step of curation might involve aggregating data sets, and rolling up summary information so that it can be easily reported on or featurized for machine learning.

Entity Resolution

Databricks Lakehouse fuels entity resolution processes that unify citizen identity or entity records and match individual payment transactions.

When bad actors attempt to defraud a government program, they usually try to alter their real identity to prevent getting caught. This is done by submitting nominally false information in the enrollment process, such as a different business name or a fake address, to reduce the potential risk of being audited by an agency fraud investigator.

With identity resolution, agencies can rapidly determine if an applicant has enrolled in entitlement programs with false information or "double-dipped" and flag the payment for investigation.

Anomaly Detection

Detecting anomalies is essential to preventing improper payments. Databricks Lakehouse supports advanced analytics with an ensemble of machine learning algorithms trained to detect suspicious transactions, which can be run against real-time events to flag potentially improper payments before they go out the door.

These models would be responsible for detecting variations in transactions, such as duplicate invoice numbers and vendor and company codes, as well as historic payments, to determine whether or not to flag a payment as potentially improper for additional human review before these payments are processed.

EBOOK

Preventing Improper Payments Before They Happen

Combating fraud, waste and abuse with data

databricks