Combating post-disaster housing recovery grant fraud

How to leverage technology to mitigate internal and external fraud

Fraud is a growing business

The Department of Housing and Urban Development (HUD) allocated $57.6 billion in Community Development Block Grant Disaster Recovery (CDBG-DR) grant funds from 2011-2019 for hurricanes, wildfires, floods, and other events.[1] The HUD Inspector General has already identified many fraud and abuse cases including bribery, public corruption, and embezzlement.[2]

Fraud is a fast-moving business requiring specialized skills and constant oversight to monitor for and stop. This article describes **ways internal and external fraudsters successfully abuse CDBG-DR grants**, preventing those who need the funds most from receiving them. It also offers ways artificial intelligence **(AI) can detect and mitigate fraud attempts** for state agencies that receive these funds.

People commit fraud. Are you prepared to stop them?

A Government Accountability Office (GAO) report suggests the $39.5 billion in CDBG-DR funds Congress appropriated for 2017-2019 may be at risk of fraud from contractors, applicants, and grantees.[3] These funds put a lot of money in the hands of state agencies to disburse quickly and monitor their use – tasks many agencies are not fully prepared to manage.

The longer funds are available, the higher the chance for fraud from internal or external parties. State agencies are under constant pressure to distribute grant funds fast. To keep up with demands, agencies often work with vendors to help disburse funds in the most efficient way. While this method works in some cases, in others, it also opens funds up to risk.

The GAO analysis in the following diagrams outlines the roles external fraudsters can play, including contractors and vendors as well as disaster assistance applicants, grantees, and their subrecipients.

Fraudsters can also be inside the organization. When agencies receive substantial amounts of funding at a fast pace, it often pushes processes to a breaking point. Outdated systems are also often unable to manage the volume of applications. Employees have access. They are also keenly aware of manual processes that rely on human eyes to spot anomalies and where controls are weak or nonexistent. Synthetic identity theft is one of the most significant fraud risk for agencies. This type of fraud occurs when fraudsters combine real and fake information to create new identities. They can use these fake identities to apply for grants on their own or collaborate with external parties to commit fraud.

Fraudsters can get away with schemes for months or years. Passing time makes it more difficult to measure the actual cost of fraud, which includes the direct monetary loss, time and expense to investigate and prosecute fraud, as well as the personal losses when funds are no longer available to go to people who need them most.

---

[1] Source: GAO, Report to Congressional Requesters, "Disaster Recovery: HUD Should Take Additional Action to Assess Community Development Block Grant Fraud Risks," May 2021.

[2] Source: House Hearing, 117 Congress, "Ensuring equitable delivery of disaster benefits to vulnerable communities and peoples: An examination of GAO's findings on the CDBG-DR program," January 19, 2022.

[3] Source: GAO, "Disaster Recovery: HUD Should Take Additional Action to Assess Community Development Block Grant Fraud Risks," May 5, 2021.

Fraud Risks of Department of Housing and Urban Development's (HUD) Community Development Block Grant Disaster Recovery (CDBG-DR) Program

Contractors and vendors

These fraud risks include bid rigging, billing fraud, and misrepresenting qualifications or eligibility.

Disaster recovery grantees and their subrecipients

These fraud risks include embezzlement and misrepresentation of impacted and distressed areas.

Disaster assistance applicants

These fraud risks include false damage claims, false eligibility claims, and falsified application documents.

General or cross-cutting

These fraud risks include collusion in contracts and bid manipulation; bribery and kickbacks; and corruption.

Source: GAO analysis. I GAO-21-177

CDBG-DR fraud examples

1. Contractor and vendor fraud

Two construction companies contracted with homeowners who received Rehabilitation, Reconstruction, Elevation, and Mitigation grants after Hurricane Sandy but performed little or no work. Their actions led to a loss of $581,691 in government funds. Both company owners pleaded guilty. New Jersey courts sentenced one to 7 years in prison and the other to 5 years of probation in addition to ordering them to pay financial restitution to their 23 victims and to the state.[4]

2. Duplication of benefits

GAO identified 500 cases of potential duplication of benefits out of 8,260 households that received CDBG-DR assistance studied. The Federal Emergency Management Agency also approved these 500 households for over $1 million in assistance.[5]

3. Disaster assistance applications fraud

A Louisiana state senator received $188,000 in Louisiana Road Home Program, Small Rental Property Program disaster recovery funds to go toward repairing his rental property. In exchange, the senator agreed to rent the property to low-income tenants at affordable rates. A U.S. district court sentenced him to four years of probation and ordered him to repay the grant in full for forged documents misrepresenting that low-income tenants occupied the property when it was actually vacant.[6]

[4] Source: Stephen M. Begg, Office of Inspector General, U.S. Department of HUD, "Civil Rights and Protections in the Federal Response to Hurricanes Maria and Harvey," June 25, 2021.

[5] Source: Kylie Bielby, Homeland Security Today, "GAO Finds Disaster Recovery Grants for homeowners are Subject to Fraud," August 22, 2023.

[6] Source: Stephen M. Begg, Office of Inspector General, US Department of HUD, "Civil Rights and Protections in the Federal Response to Hurricanes Maria and Harvey," June 25, 2021.

AI can make a difference

Adding controls that use AI can help monitor actions associated with grant use, including who withdraws the funds, what contractors the recipient secures, lease applications and agreements, and construction permits applied for related to the grants. This critical monitoring can flag potential fraud and might have mitigated these three CDBG-DR fraud examples.

Many state agencies do not have data scientists on staff to identify and stop fraud. Having someone in this role is critical, and today's technology capabilities can help. For example, predictive modeling using computer vision and natural language processing (NLP) can identify patterns and trends in text- and image-based data to detect fraud. AI and other advanced technologies, such as the following, can be valuable tools to add controls that monitor internal and external fraud risks in CDBG-DR programs.

- **Predictive analytics:** By analyzing historical data, AI can identify trends and patterns that are indicative of potential fraud. This can help authorities proactively identify and prevent fraudulent activities before they occur.
- **Risk assessment:** AI can assess grant application risks by analyzing factors such as the applicant's financial history and relationship with other involved parties. This can help identify high-risk applications that may require additional scrutiny.
- **Fraud detection:** AI algorithms can analyze large volumes of grant management-related data, including financial records, applications, and documentation, to identify patterns and anomalies indicative of fraudulent activities. By flagging suspicious cases, AI can help authorities prioritize their investigations and take appropriate actions.
- **Compliance monitoring:** AI can assist in monitoring compliance with grant management regulations and policies. By analyzing data and documentation, it can flag inconsistencies or non-compliance issues such as duplicate claims or misallocated funds.
- **Real-time monitoring:** AI can continuously monitor transactions and activities related to grant management to look for suspicious or abnormal behavior. This can include monitoring financial transactions, vendor relationships, and unusual changes in project plans or timelines.

Spot what's different

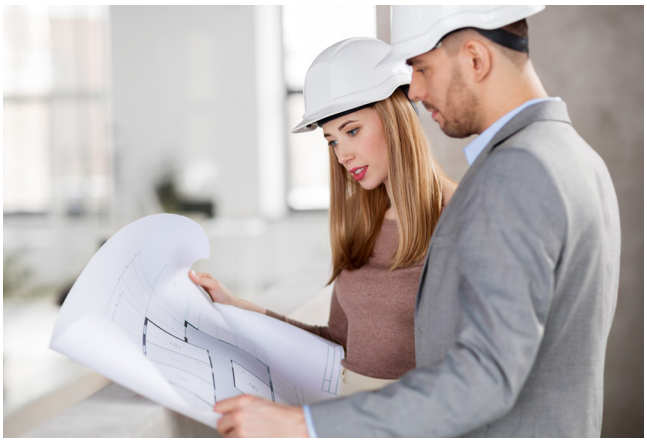
One of the most effective methods to recognize fraud is identifying anomalies. AI can process and analyze large amounts of data quickly and accurately to find anomalies that can reduce CDBG-DR program fraud as described in these examples.

1. **Extracts/integrates data:** Using AI to integrate data from documents such as contracts, invoices, and site inspection reports into a unified dataset allows a comprehensive information analysis and comparison. AI detects whether the document is machine-readable as well as its type to determine what pipeline to use to extract information. The method used to process each will depend on the type of document. AI also takes data from unstructured to structured format and combine it across data sources.
2. **Recognizes patterns:** AI algorithms learn patterns and relationships within the data, enabling them to identify discrepancies or anomalies. These algorithms identify inconsistencies between what the contract states, what the invoice documents, and what the site inspection reports. They also find price and overtime differences across facilities, vendors, and other sources.

3. **Uses natural language processing to understand text:** AI analyzes and understands text within contracts, invoices, and inspection reports. This comprehension helps identify language discrepancies such as conflicting terms or ambiguous clauses. NLP helps find scope of services and terms similarities across contracts and vendors. It also identifies contract elements that make contracts or vendors unique compared to their benchmark group. NLP also helps extract unstructured data based on sentence context and key words to identify relevant information to extract.
4. **Automate for efficiency:** Using AI to automate anomaly detection can significantly reduce the time and effort required to manually compare contracts, invoices, and inspection reports. Automation allows faster discrepancy identification and more timely issue resolution. It can create automated Microsoft Word-based reports summarizing investigation findings and investigative team schedules to optimize travel time between sites. Machine learning can stratify facilities into risk groups, which can guide agencies on what facilities they should visit next based on past findings from field and data in invoices and contracts.

Helping you mitigate fraud

Fraudsters will continue to find new and innovative ways to introduce fraud into CDBG-DR grant programs. KPMG applies leading-edge analytical techniques, AI, emerging technologies, and a mature framework to help state and local governments with identifying, mitigating, and protecting against fraud. Our teams have implemented anti-fraud models in state environments in two-to-three weeks. In addition, our KPMG Smart Grants Platform employs automated data validation tests that are designed to detect instances of fraud and duplication of benefits, helping ensure accurate, efficient, and compliant CDBG-DR grant review processes in accordance with funding agency regulations.



Contact us

Thomas Stanton
Principal, Forensic
KPMG LLP
T: 218-872-7758
E: tstanton@kpmg.com

Bobby Gorantla
Managing Director, Data & Analytics
KPMG LLP
T: 717-260-4775
E: bgorantla@kpmg.com

Andrew Neville
Senior Manager, Economic and Valuation Services
T: 703-286-2913
E: aneville@kpmg.com

Learn more: visit.kpmg.us/recovery

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia