mastercard

Agency leaders playbook: new tools for achieving card program success

New analytical technologies and payment solutions are emerging to help agency leaders fight against fraud, bring more transparency into the procurement process, and achieve cost-savings associated with purchases.

Fraud, waste, and abuse pose significant risks to the integrity of an agency or an organization and can erode public trust in government. According to the Government Accountability Office (GAO), government fraud and improper payments totaled $136.7 billion in FY 2015, a $12 billion increase over the previous year.

Modern analytics technologies and payment solutions are allowing federal financial leaders to detect high-risk transactions and patterns of misuse.

Separately, in a report published in May 2017, GAO reported noted losses at one agency due to contractors' improper use of government purchase cards, exploiting weaknesses in the agency's internal controls system.

A recent Government Business Council (GBC) survey of federal financial leaders — Financial Data Management in the Federal Government — indicates that inefficient systems continue to challenge financial management processes. Nearly half of the federal respondents expressed either low or no confidence in the capabilities of current systems to detect and mitigate improper payments due to fraud and abuse, according to the survey of 152 civilian and defense federal financial leaders.

Outdated software inhibits current fraud fighting capabilities, according to the survey. One-third of respondents cited difficulties in drawing conclusions from data, while nearly as many cite inefficient manual reporting processes opening the door for error and duplication of labor.

Fighting fraud, waste and abuse

However, agencies can combat fraud, waste, and abuse by implementing risk management best practices and improving anti-fraud analytics. Modern analytics technologies and payment solutions are allowing agency leaders to detect high-risk transactions and patterns of misuse.

In July 2015, to preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks and organized them into a conceptual framework called The Fraud Risk Management Framework (the Framework).

"The Framework encompasses control activities to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks," according to the GAO. In addition, the Framework lists four components needed to effectively manage fraud risks.

Those four components are:

1. **Commit**—Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
2. **Assess**—Plan regular fraud risk assessments and evaluate risks to determine a fraud risk profile.
3. **Design and Implement**—Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
4. **Evaluate and Adapt**—Evaluate outcomes using a risk-based approach and adapt

activities to improve fraud risk management.

To detect and prevent fraud, waste, and abuse, federal financial leaders must design and implement specific control activities, including policies, procedures, techniques, and mechanisms. In addition to designing and implementing new control activities, financial leaders must also revise existing control activities if they determine that certain controls are not effective in reducing or preventing fraud risk.

Preventive activities generally offer the most cost-effective investment of resources to mitigate fraud, waste, and abuse, according to the GAO. Moreover, automated control activities such as automated data-analytic techniques tend to be more reliable than manual control activities such as document reviews. Automated controls are typically less susceptible to human error and are more efficient. The GAO Framework identifies certain control activities that are broadly applicable to any federal agency risk management program.

The controls include:

- data analytics activities,
- fraud awareness initiatives,
- reporting mechanisms, and
- employee integrity activities.

Data Analytics

Data analytics activities can include a variety of techniques. "For example, data mining and data matching techniques can enable programs to identify potential fraud while predictive analytics can identify potential fraud before making payments," according to the GAO.

The federal government advises agency financial leaders to take a risk-based approach to data analytics and consider the benefits of implementing specific data-analytic tools and techniques while also assessing the support the program will need. This means making sure employees have sufficient knowledge, skills, and training to perform data

GAO recommends that financial managers conduct the following data analytics activities to prevent and detect fraud:[1]

- Apply system edit checks to help ensure data meet requirements before data is accepted into the program's system and before payments are made.
- Conduct data matching to verify key information, including self-reported data and information necessary to determine eligibility.
- Conduct data mining to identify suspicious activity or transactions, including anomalies, outliers, and other red flags in the data.
- Automate data-analytic tests to monitor data for fraud indicators on a continuous basis.
- Tailor the output of data analytics to the intended audience to help ensure the results are usable.
- Review the results of data analytics and refer appropriate cases to the Office of Inspector.

analytics.

Agency leaders should combine data from multiple sources and databases within the agency to facilitate reporting and analytics. At the same time, financial managers should seek access to necessary external data, including pursuing data-sharing agreements. They must consider program rules and known or previously encountered fraud schemes to design data-analytic tests.

Insights On Demand, exclusively for Mastercard

Mastercard is offering a data-analytical solution – Insights On Demand (IOD) that is uniquely designed to help address the requirements described in GAO's Framework for managing risk associated with card transactions. IOD helps to detect fraud, waste, and abuse, within card programs including purchase, travel, fleet and integrated cards. IOD is available to agencies through SP3 and through their selected SmartPay 3 Issuing financial institution, if they select Mastercard.

IOD identifies high-risk transactions or patterns of misuse. Financial managers can view outliers by spend category, merchants and employee as well as detect split purchases that circumvent transaction limits. IOD targets those expenses with suspicious keywords or phrases and identifies duplicate card submissions. The analytical solution detects excessive and suspicious activity, identifies duplicate or unusual mileage activity, and recognizes geographic areas with high numbers of suspect transactions.

Financial managers can flag outliers by spend category, merchants and employee as well as detect split purchases that circumvent transaction limits.

IOD is applying evidential reasoning, a form of artificial intelligence, and machine learning technologies that assist agencies and organizations in identifying employee and consumer purchasing patterns. Machine learning or self-teaching systems analyze historical transaction data to help detect fraudulent patterns.

IOD incorporates sophisticated filtering and drill-down capabilities to facilitate analysis and data export to Microsoft Excel and other standardized formats. Also, agency users can generate standard and ad hoc reports based on their choice of variables.

Using IOD, agency leaders can assist in investigating alleged wrongdoing or suspected fraud, waste, or abuse by agency or organization employees, or those entities doing business with the federal government or tribal organizations.

Improving transparency

Legislation, guidance by the Office of Management and Budget (OMB), and new internal control standards focus on the need for program managers to take a strategic approach to managing improper payments, risks, and fraud. By implementing a strategic, risk-based approach and developing antifraud controls combined with the right type of technology, financial leaders and agency program managers can be more proactive in eliminating fraud, waste, and abuse. Government agencies are looking for ways to **improve the transparency** of purchases to increase efficiency and reduce fraud. Federal financial leaders need better visibility into how government employees are purchasing goods and services — whether that is buying printer ink or expensing travel costs. Agencies are now required — via the Digital Accountability Act — to make their spending information public on USASpending.gov.

Citizen expectations for greater transparency in government continues to rise, making

it even more important to make data accessible — both for taxpayers as well as the financial officers and stakeholders in charge of managing the government's massive troves of financial data.

Despite this urgent need, 40 percent of federal financial leaders who responded to the GBC survey describe access to financial data at their organization as less than satisfactory. By continuing to press for standardized data formats and emphasizing a data-centric culture, agencies will be in a much better position to justify their spending data and correct lingering deficiencies related to inaccurate reporting, the survey shows. It's clear that current systems and processes require reforms to ensure they can detect and mitigate fraud, waste, and abuse triggered by employee misuse of funds. Improving current data analytics and integrating leading practices in fraud management such as those detailed in GAO's Fraud Risk Management Framework and OBM's guidelines will help agencies save money, allocate more responsibly, and ensure greater integrity in pursuit of their mission, according to the GBC report.

Improving visibility and security

Financial leaders can gain more visibility by leveraging Electronic Accounts Payable or single-use-account numbers. For example, Mastercard can offer In Control® for Commercial Payments (ICCP) as a virtual card account solution.

ICCP is an industry-leading solution built to help streamline and automate payments. Unique, dynamically generated virtual account numbers help make sending payments to suppliers flexible, easy, and secure.

Agencies and organizations can get the advantage, flexibility, security, visibility, and traceability of a single-use virtual-card number. A new number is generated for each transaction, providing each transaction a unique identifier.

Transaction controls can be set, and reconciliation is automatic, greatly improving security. Virtual payments are supported by the same proven, trusted infrastructure that supports traditional credit cards. There are various implementation models, so an agency or organization does not need to overhaul its entire procurement process to begin using virtual payments.

ICCP in action:

Controls: Managers configure employee privileges including approved purchase categories, limits, alerts, and workflow escalation path.

Purchase: Employees submit purchase requests and invoices for approval, which are delivered through an automated workflow to the supervisor.

Payment: Upon approval, the solution generates a limit use Virtual Card number for the employee to complete payment.

Reconciliation: Solution reconciles the unique Virtual Card Number upon settlement and generates a report for easy access.

Achieving savings and rebates

GSA's Center for Charge Card Management administers the SmartPay charge card program, which includes purchase cards for supplies and services; travel cards for airline, hotel, and related travel expenses; fleet cards for fuel and supplies for government vehicles; and integrated cards for a combination of purchase, travel or fleet cards. In addition to improving transparency and reducing fraud, waste, and abuse, card programs help agencies to derive **significant cost savings.**

The replacement of paper-driven acquisition processes of the past with the use of purchase cards saves the government about $1.7 billion annually in administrative costs, according to the General Services Administrations' (GSA) SmartPay website.

The replacement of paper-driven acquisition processes of the past with the use of purchase cards saves the government about $1.7 billion annually in administrative costs, according to the General Services Administrations' (GSA) SmartPay website.

By implementing Electronic Account Payable solutions, an agency can yield even more cost savings and opportunity for additional rebates. Agencies have the opportunity to increase refunds by having more cards per account; more spend per card, and new volume from replacing other payment methods. Designing a best in class program can provide opportunities for incremental returns.

As new analytical tools and payment solutions emerge, federal financial leaders have the opportunity to gain additional efficiencies and refunds by:

- Continuing to digitize the payment processes, including invoices and approvals.
- Using Big Data analysis to gain better insight into fraud, waste, and abuse, and to improve financial forecasting.
- Optimizing existing cards program and expanding the use of virtual cards.

For more information or to request a demo on Mastercard SmartPay 3 solutions, please contact your Mastercard account representative.

Source

1 GAO, Fraud Risk Management Framework