How to Combat Government Fraud, Waste, and Abuse:

Getting Started Guide

By John Verver, CA, CMC, CISA, Vice President, Strategy, ACL

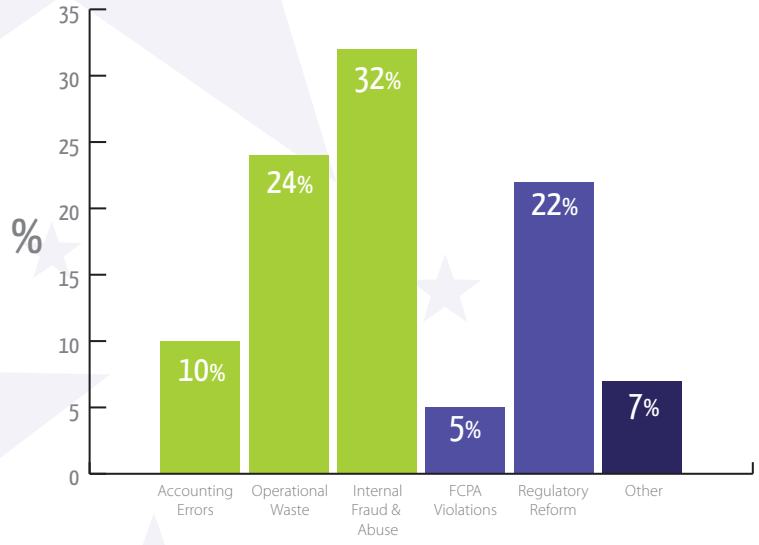
How to Combat Government Fraud, Waste, and Abuse: Getting Started Guide

By John Verver, CA, CMC, CISA, Vice President, Strategy, ACL

A REALLY BIG PROBLEM

It is no secret that government bodies around the world face an enormous problem in fraud, waste, and abuse. For example, the U.S. Government Accountability Office estimates improper payments totaling well in excess of $100 billion annually at the U.S. federal level alone.

Many of the abuses take place within government programs such as unemployment insurance, healthcare, and social security. Others take place within major contract procurement systems for the military, transportation infrastructure, and education. Many instances of government fraud and waste are no different to those that take place in any corporation or for-profit organization where there is a constant risk of employee wrongdoing. Improper payments can occur in a wide range of ways and in the vast majority of systems.



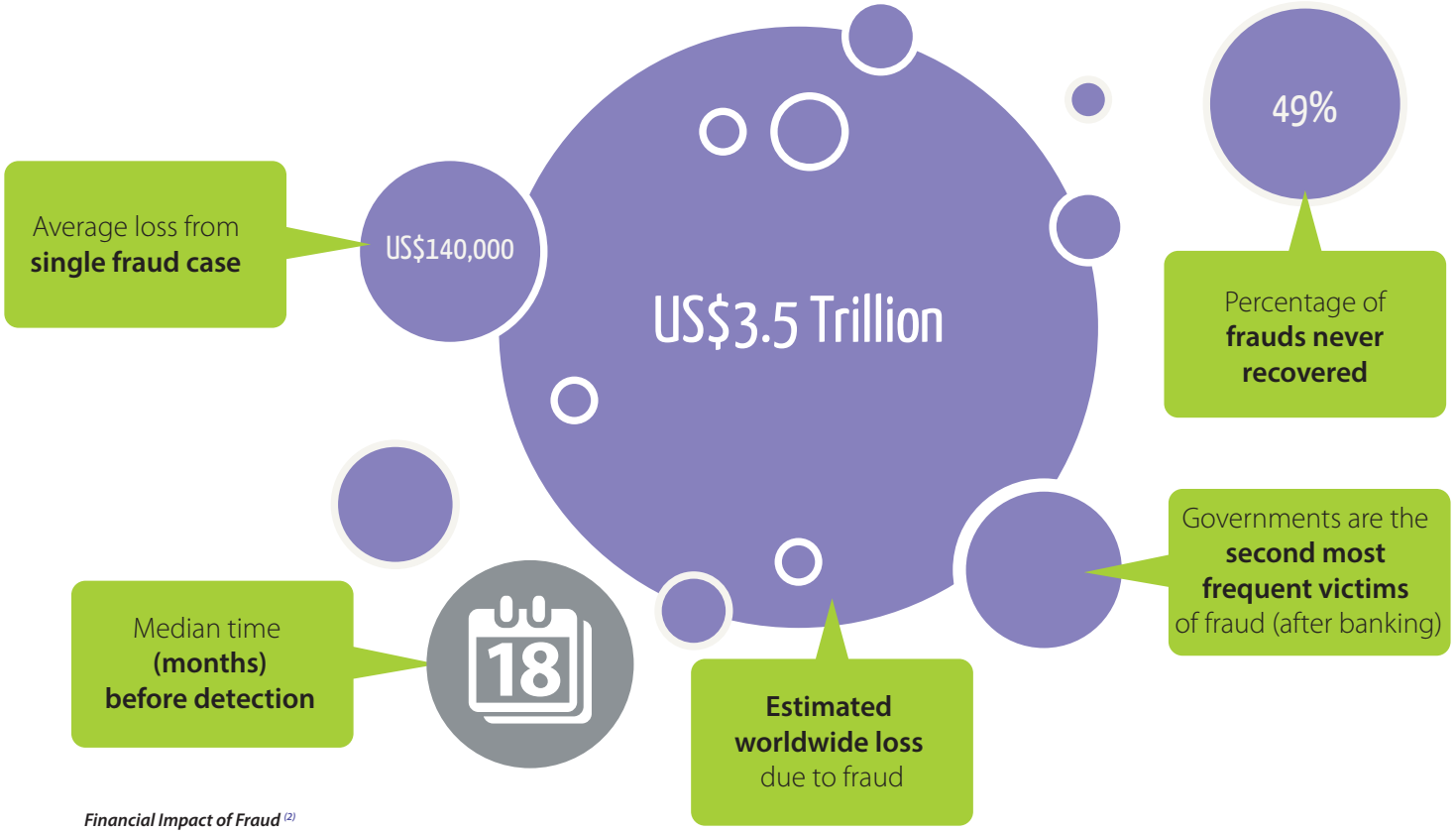
Largest Concerns for 2014 [1]

So, what can you do to better protect public funds?

The ideal solution to government fraud, waste, and abuse would see a comprehensive system of policies, procedures, and controls effectively thwarting all occurrences of improper payments, whether by government employees or the beneficiaries of government programs. In the real world, of course, it is just not possible to prevent all such instances. Risks always exist, control systems are never perfect, and both systems and people are fallible.

On the other hand, detection of instances of fraud, waste, and abuse that have taken place is a much more feasible objective. Even in the most complex system with many millions of transactions and massive monetary amounts involved, a data trail exists in some way or another of virtually every instance of any improper payment. This is where technology, specifically data analysis software, has a critical role to play. By analyzing entire populations of transactions and associated data to look for a variety of indicators of fraud, waste, and abuse, data analysis can identify where problems have occurred. Once the nature, extent, and details of the problems are known, it is then possible to address them and plan to prevent their recurrence.

[1] *Association of Certified Fraud Examines (ACFE), 2012 Report to the Nations on occupational Fraud and Abuse*



Financial Impact of Fraud [2]

> WE DON'T HAVE A FRAUD PROBLEM."
> **– FAMOUS LAST WORDS**

There is a tendency in many organizations, particularly those within the high-performance category, to assume that fraud only happens elsewhere. Unfortunately, the reality is that in almost every organization there are going to be employees who seek to benefit themselves at the expense of their employer. P-Card and T&E abuse are areas in which fraudsters can most easily rationalize their actions, sometimes not even considering their abuse to be fraudulent. Other realities are that even the most well intended policies will be ignored and that no internal controls are ever perfectly effective.

Purchasing cards (P-Cards) and travel and entertainment (T&E) expenses are both areas in which the use of technology, specifically data analysis software, has a critical role to play in identifying indicators of fraud and stopping fraudsters in their tracks. Both are areas that typically involve very large volumes of transactions. At the same time, effective controls in both areas usually depend upon regular approvals by appropriately authorized individuals. What often happens is that, over time, review and approval processes become less stringent and effective. Employees are often quick to realize that this is happening and learn ways to further circumvent an increasingly weak control system.

Fortunately, this situation is one in which data analysis can be particularly effective. By analyzing millions of transactions and looking for a variety of indicators of fraud, data analysis can make up for control weaknesses and rapidly identify where fraud has occurred.

In this eBook, we'll show you how.

[2] *Association of Certified Fraud Examines (ACFE), 2012 Report to the Nations on occupational Fraud and Abuse*

HOW IS DATA ANALYSIS USED TO DETECT GOVERNMENT FRAUD, WASTE, AND ABUSE?

Let's take a look at how data analysis can help deal with the problem overall, as well as in some of the most common areas in which government fraud, waste, and abuse typically occur.

There are two primary ways in which data analysis is generally used to detect a broad range of types of fraud, waste, and abuse.

01. The first is to **analyze entire populations of transactional data to look for various forms of statistical or other anomalies**. This does not necessarily prove that fraud or abuse has actually occurred, but it can be a very effective way of highlighting a situation that just does not seem to make sense and warrants further investigation.

Why, for example, should one government contractor, providing essentially the same goods and services as a hundred others, be paid 50% more than the average? There could be several valid reasons why this could be justified. But if no reasons are obvious, then it could be a valid indicator that there is an increased risk of fraud having occurred.

02. The second and more specific approach is to **analyze transactions for indicators of known risks of fraud, waste, and abuse**. An employee may be authorized, for example, to use a Procurement Card (P-Card) for purchases of specific business items. If an analysis of P-Card data shows that a series of purchases were made from a home renovation store, this could be a strong indication of an actual fraud.

The (in)dispensable spreadsheet

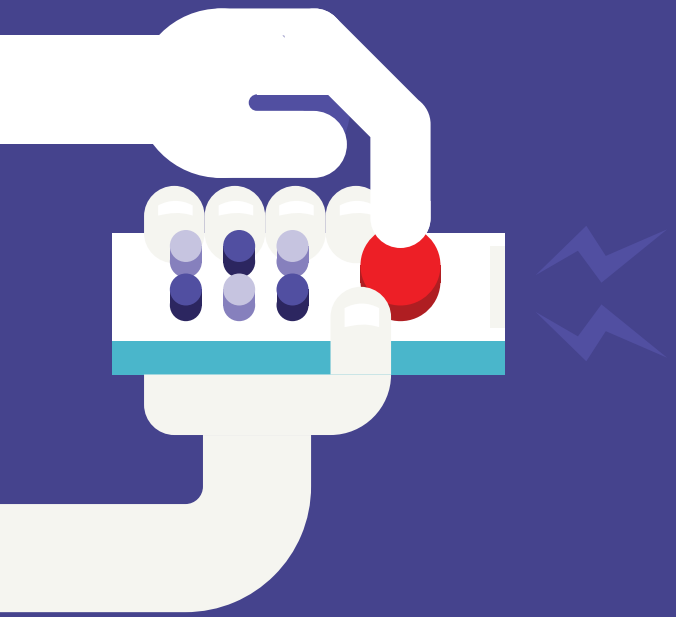
For those involved in fraud detection, the ease-of-use, adaptability, and low cost of spreadsheets may make it a strong draw. Beware. Organizations need to balance the appeal of spreadsheets against their shortcomings, including:

- **Lack of data integrity** – values may be altered deliberately or accidentally
- **Error prone** – errors in input, logic, data interfaces, and use
- **Not in line with standard IT regimes for critical applications** – documentation, testing, and version control
- **Hard to duplicate results** – no standard process and no audit trail

The problem is the business world's over-reliance on spreadsheets. There is a time and a place for spreadsheet use–but when it comes to fraud detection, consider making the spreadsheet dispensable in your organization.

How smart is Business Intelligence (BI)?

Generic BI tools are very good at providing high level reports and summaries, but fall short at the type of detailed analysis and testing of individual transactions that are needed to deliver fraud warning signs.



ERP CONTROLS ≠ FWA PROTECTION

Some organizations believe that they are protected from fraud, waste, and abuse (FWA) by control mechanisms in their organization's enterprise resource planning (ERP) systems; however, this is usually insufficient for effective fraud detection and prevention. Built-in controls in ERP systems often get turned off, for a variety of reasons, or can be circumnavigated.

ERP systems are also usually unable to compare information from other business systems to look for red flags, for example to compare employee information from HR systems with vendor records. That's why you need to test for suspicious transactions and patterns with software that is independent of operational systems through which your transactions flow.

FRAUD DETECTION TECHNIQUES IN PRACTICE

One of the most effective data analysis techniques is to compare data across different databases and systems—often in ways that are never normally compared. One simple example is to compare procurement and payments information with human resources (HR) records (e.g., bank account and other personal data) to see if there are indications of an employee having set up a "phantom vendor" scheme, paying invoices to a made-up vendor at their home address.

Another type of data analysis involves testing to see if enterprise resource planning (ERP) application control settings, or master file data, have been changed in a way that indicates potential fraud and abuse. What if a manager was authorized to approve purchase orders (POs) up to $5,000—but a change had been made to the system so that this limit was increased to $50,000, perhaps just for a few hours before the change was reversed?

Around the world, internal auditors, risk management, and compliance professionals are using data analysis to help transform their effectiveness. Government auditors and inspector general offices have the same opportunity. However, no matter whether private or public sector, surveys of risk and controls professionals all indicate the same thing: exponentially growing data means that data analysis needs to be tapped far more extensively than ever.

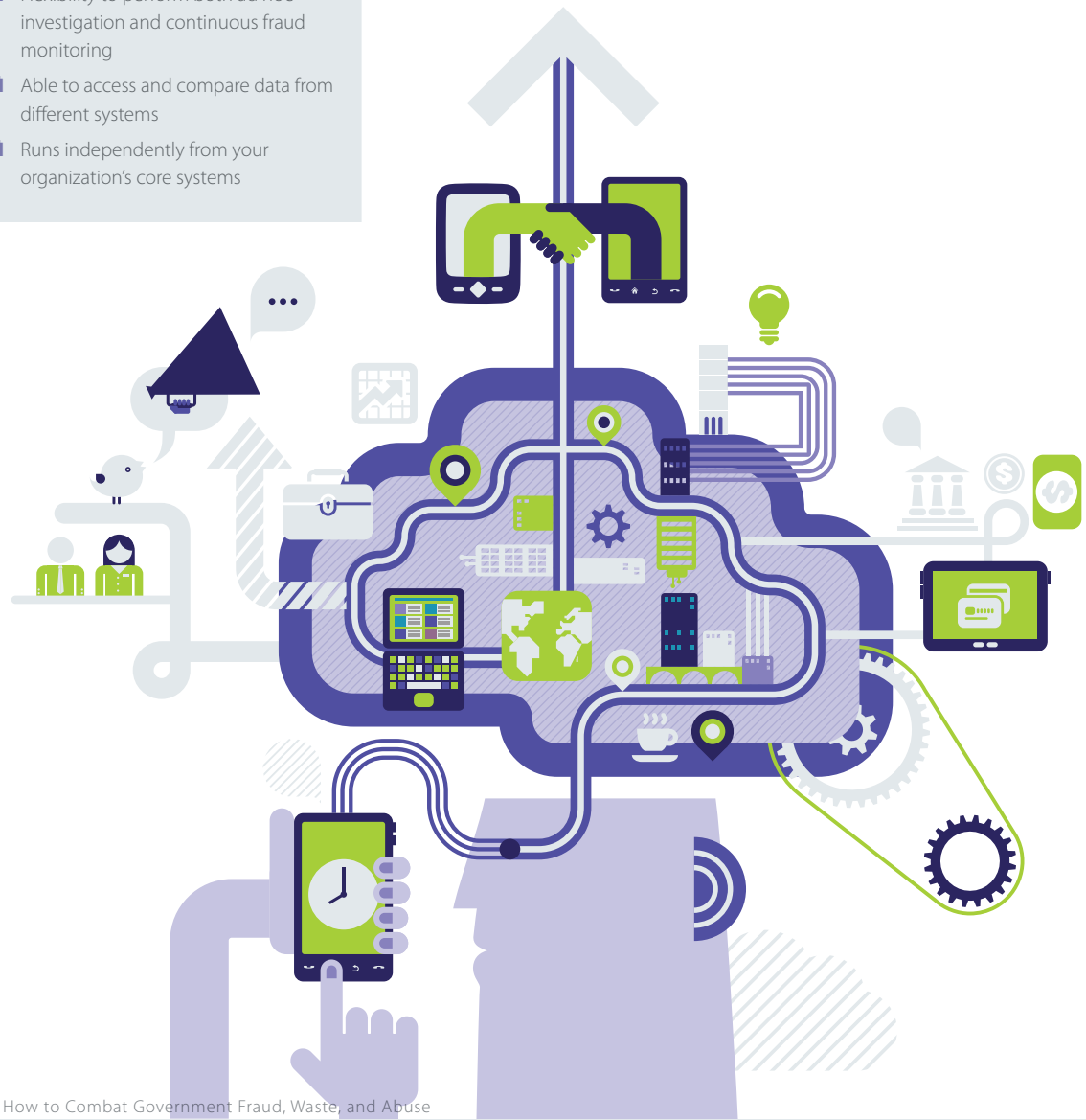
TO SAMPLE OR NOT TO SAMPLE?

There can be a valid role for sampling in audit and control testing, but it is not an effective approach for automated fraud detection and prevention. The great benefit of using data analysis is that it allows every transaction in a population to be rapidly examined and tested for fraud. It can provide immediate quantification of the likely extent of different types of fraud and show patterns and trends that may indicate changing fraud risk profiles.

FRAUD DETECTION SOFTWARE MUST-HAVES CHECKLIST:

- ❑ Performs procedure logging
- ❑ Flexibility to perform both ad hoc investigation and continuous fraud monitoring
- ❑ Able to access and compare data from different systems
- ❑ Runs independently from your organization's core systems

A LOOK UNDER THE HOOD: SOFTWARE FOR DETECTION OF GOVERNMENT FRAUD, WASTE, AND ABUSE



Data analysis software designed specifically for detection of fraud, waste, and abuse has specific functional capabilities. In general, these capabilities are similar to those for data analysis in audit or for other risk and control testing purposes.

Pre-built analytic routines, such as classification, stratification, duplicate testing, aging, join, match, compare, as well as various forms of statistical analysis, all have a role to play in helping to find fraud indicators. Data visualization is another useful capability, particularly for helping to spot unexpected anomalies and to provide new insights. Software also needs to have a high degree of flexibility to support full automation and the development of complex tests that address the sophistication of some fraud detection requirements.

One important capability to look for in data analysis software for both audit and fraud detection is that of logging of all procedures performed. This can prove to be of importance in generating complete audit trails that may be required to support detailed investigation and possible subsequent prosecution.

In practice, another of the most critical capabilities of data analysis technologies for audit and fraud detection is the ability to access a broad range of data. As indicated previously, there may be a requirement to compare data from a range of data sources, both internal and external. The technical structure of data from different sources may vary considerably. Specialized fraud and control testing software should include the ability to access and combine data in ways that are not commonly available in more general purpose analysis software.

MANAGING THE ENTIRE FRAUD, WASTE, AND ABUSE DETECTION PROCESS

Although our focus in this eBook is on the critical role that data analysis plays in effective fraud detection, management of the entire fraud detection process also plays an important role—as does supporting the overall risk management process in which fraud should be considered among the risks that need to be addressed.

P-Card and T&E expense fraud are specific fraud risks that should be considered and addressed as part of the risk management process. The following are the key elements of a general model for an overall risk management process. Beyond fraud detection capabilities, your software needs to support all of these components:

LOW HANGING FRUIT: DATA ANALYSIS QUICK WINS OVER IMPROPER PAYMENTS

Fraud, waste, and abuse in government can occur in almost any of the areas encountered in the private sector. Problems and risks in government programs for Medicare / Medicaid, unemployment insurance and infrastructure development have a lot in common with those that occur in industries such as healthcare, insurance, and construction. Functional process areas, such as procure-to-pay (P2P), payroll, procurement cards (P-Cards), and travel and entertainment (T&E) expenses operate almost identically in the public sector as in companies. The techniques for analyzing data and testing for fraud and control problems are also similar.

There are literally thousands of different fraud and waste data analysis tests that are in use across government organizations around the world, addressing a very wide range of risk and control issues. Most organizations start their use of audit and fraud detection analytics in the common process areas, often because this is where the quick wins usually occur.

The following sections look at some specific areas and describe the types of data analysis that detect some typical instances of improper payments in P-Cards, T&E expenses, and government programs.

P-Card

HOW TO IDENTIFY EMPLOYEES' FRAUDULENT USE OF PURCHASING CARDS

Purchasing cards (P-Cards) are increasingly used by government organizations to reduce the costs of traditional procurement processes.

While this makes a lot of sense in terms of efficiency and effectiveness, P-Cards are particularly prone to fraudulent use because they are so easy to use. An employee may also realize that review and approval processes have become lax and use P-Cards in a variety of ways that provide personal benefit at the expense of the organization.

Any chance I can expense this cow?

An example of an actual P-Card fraud is a manager in a district branch of a telecommunications company who used his P-Card to pay for **cattle bought at an auction for his hobby farm**. He knew that his card usage was not reviewed in detail by senior management. The fraud came to light when data analysis was used to identify a purchase made at a weekend and for a non-standard merchant code.

VS

Just because it looks like a fraud doesn't necessarily mean it is…

Of course, while data analysis can provide a good indication of a suspicious activity, it is always important not to jump to conclusions without appropriate investigation. We know, for example, of a case in which transaction monitoring identified a **police officer purchasing alcohol at a liquor store with an official credit card**. It turned out that the officer was teaching a breathalyzer usage course and needed the alcohol for demonstration purposes. It would not have been a good idea to accuse the officer of fraud!

PURCHASING CARD FRAUD TESTS

The following are examples of some common data analysis tests used to identify indicators of employees' fraudulent use of P-Cards.

Issue: Purchases of items intended for personal use

One of the most common abuses is to use P-Cards for goods and services that are not for legitimate business purposes

Tests:

- ❑ Analyze transactions to look for merchant codes, vendor names and key words that are associated with non-business items and services
- ❑ Identify transactions made on weekends, holidays or while the employee is on vacation
- ❑ Identify split transactions in which a large purchase is paid for in smaller amounts, just under a review/approval threshold

Issue: Duplicate purchases

There are a variety of ways in which P-Cards can be used to duplicate purchases to the benefit of the employee.

Tests:

- ❑ Identify multiple purchases of the same item or service within a specific timeframe. One purchase may be legitimate, the other may be intended for personal use
- ❑ Identify where a P-Card was used for a specific purchase and the same purchase was processed as a T&E claim

Issue: Unusual usage patterns

Unusually high or frequent use of P-Cards can indicate a potential fraud.

Tests:

- ❑ Look for P-Card holders whose usage is abnormally high—both in cost and frequency—compared to others in a similar role
- ❑ Identify P-Card holders with unusually large cost limits on their cards

Issue: Fuel cards

Fuel cards are effectively a form of P-Card and are particularly prone to abuse. Employees may use a fuel card to fill vehicles of friends and family or even separate fuel tanks that are intended for personal use.

Tests:

- ❑ Look for fuel card usage that is abnormally high compared to others in a similar role
- ❑ Calculate expected mileage for a particular volume of fuel charged and compare to typical or expected travel patterns

SLEEP TIGHT, DON'T LET THE FRAUDSTERS BITE

- An inspector general's office identified abuse by one cardholder charging more than 1,000 hotel nights in a single year, amounting to US$120,000.
- One customer discovered a staff member booking first class flights for business travel, and then exchanging the ticket for an economy fare after the expense had been submitted—leaving him a credit with the airline that he used for personal vacations.

BUT, ALL THE OTHER SENATORS ARE DOING IT...

- Beginning in late 2012, Canadian taxpayers began to learn about a long-lasting political scandal concerning the expense claims of several Canadian senators, who claimed travel and housing expenses for which they were not eligible. This triggered an investigation of the expense claims of the entire Senate by the Auditor General of Canada, identifying ineligible claims by some senators totaling hundreds of thousands of dollars each.

HOW TO IDENTIFY EMPLOYEES' FRAUDULENT TRAVEL & ENTERTAINMENT EXPENSES

Employee fraud in the area of Travel and Entertainment (T&E) expenses can include a broad range of types.

In government organizations in which employees are provided with credit cards for T&E usage, the types of fraud, and the ways to identify them, can be very similar to those for P-Cards. In some cases, organizations provide credit cards to employees for use both in purchasing goods and services and for travel and entertainment expenses. In other cases, employees submit expense reports for reimbursement. Both methods are rife with opportunity for fraud and error.

TRAVEL & ENTERTAINMENT FRAUD TESTS

The following are examples of some common data analysis tests used to identify indicators of employees' fraudulent Travel and Entertainment (T&E) expense claims.

Issue: Claims for personal expenses

One of the most common abuses is for expense claims that are not for legitimate business purposes. Government employees, particularly those who travel frequently, may be tempted to charges for personal use airfares, hotel and meals, knowing that it may be hard for an approver to recognize when a trip was for personal rather than business purposes.

Tests:

- ❑ Identify expenses relating to airfares and hotels in non-standard locations (e.g., exotic resorts)
- ❑ Identify expense claims including vendor names and key words that are associated with non-business items and services
- ❑ Identify expense claims for periods when the employee is on vacation

Issue: Duplicate claims

There are a variety of ways in which fraudulent duplicate T&E claims can occur.

Tests:

- ❑ Identify claims for meals for multiple persons made on the same day and at the same location as claims made by other employees
- ❑ Identify expenses incurred using both a company credit card (P-Card or general corporate card) as well as through a reimbursement claim

Issue: Unusual usage patterns

Unusually high or frequent T&E expense claims can indicate a potential fraud.

Tests:

- ❑ Look for patterns of unusually large T&E claims compared to employees in a similar role

Issue: Refunded or inflated expenses

A relatively common T&E fraud involves employees paying for or claiming flights, conferences or training courses through a T&E system and then cancelling the transaction. Instead of reversing the T&E charge, the employee receives the refund amount personally. Another fraud involves booking and charging for a business class ticket and subsequently changing to an economy ticket, receiving the refund personally.

Tests:

- ❑ Identify airfare payments/claims for which there are no corresponding hotel or meal charges
- ❑ Identify claims for out-of-town conferences or courses with no corresponding T&E charges

Issue: Car mileage claims and gas expenses

A variety of fraudulent schemes relate to car travel expenses. They range from over-stating mileage to duplicate claims of both mileage and public transport or car rentals.

Tests:

- ❑ Identify instances where mileage claims were made for the same time period as car rental charges or other transport costs
- ❑ Identify total car mileage claims and compare to distances of reported business travel destinations
- ❑ Identify instances where claims for mileage and gas are both made in the same time period

HOW TO IDENTIFY PROGRAMS FRAUD

As in most countries, a very large number of Federal Government programs exist in the U.S., providing a broad range of entitlements, benefits, and subsidies to organizations and individuals.

Recently, the amounts of such payments in the U.S. totaled well in excess of $1 trillion per year. The nature of many government programs makes them particularly susceptible to fraud, waste, and abuse. New and recently changed programs often create circumstances in which unforeseen risks arise for which no effective controls have been implemented.

The use of data analytics and continuous monitoring, as well as software for risk and control management, plays a vital role in helping to reduce and contain the amounts of improper payments that inevitably occur.

High-Error Programs

The U.S. Office of Management and Budget has designated 13 programs as having high amounts of improper payments. Here are the top five:

Program	Total Payments ($Billion)	Improper Payments ($Billion)	Improper Payment Rate %
Medicare fee-for-service	349.7	29.6	8.5
Medicaid	271	19.2	7.1
Medicare Advantage (Part C)	115.2	13.1	11.4
Earned Income tax credit	55.4	12.6	22.7
Unemployment insurance	90.2	10.3	11.4

Source:
http://www.fedtechmagazine.com/article/2013/08/how-federal-agencies-track-down-improper-payments-smart-data-management

PROGRAMS FRAUD TESTS

The following are just a few examples of the many types of analysis tests that can be applied to specific government programs in order to detect instances of fraud, waste, and abuse.

01. Medicare/Medicaid

Issue: Phantom Billing or Upcoding

Healthcare providers may be billing for procedures not performed or inappropriately using upcoding. One way to identify the occurrence of potential phantom billing or inappropriate upcoding is to compare the distribution of billing codes to other healthcare providers of similar size or type.

Tests:

- ❑ Identify providers having an unusual distribution of billing codes, compared to providers of a similar size/type.
- ❑ Identify providers with a higher ratio between upcodes and other billing codes.

02. Unemployment Insurance

Issue: Identity Theft and Impostors

Personal information is stolen and used inappropriately to apply for benefits. A key indication for this behavior is to identify unusual patterns in beneficiary addresses.

Tests:

- ❑ Identify benefits paid to multiple addresses for the same social security number.
- ❑ Identify benefits paid to more than x different addresses within a short time period.

03. Income Tax

Issue: Inflated, inappropriate, or fictitious deductions

Distributions of the first digits of numbers on a tax return should follow Benford's law, but often the number of values is not large enough for statistical relevance. Instead, an unusual distribution pattern of the numeric digits within the values on filed returns can be an indication of inflated, inappropriate, or fictitious deductions.

Test:

- ❑ Numeric Digit analysis: Calculate the distribution of frequencies of digits used in the tax return, and identify unusual distributions of numeric digits. For example, identify returns with the largest ratio of zeros to other digits as a criteria for judgmental sampling.

Issue: Sole Proprietorships misused to conceal and misdirect income / deductions

Sole proprietorships can be used to conceal or misdirect income and/or deductions inappropriately.

Test:

- ❑ Sole Proprietor Industry Metric Analysis: Calculate key metrics for sole proprietors based on industry codes, such as income/expense/equity ratios and cash ratios. Flag sole proprietors that have unusual metrics compared to similar sole proprietors of the same industry code.

TAKING FRAUD DETECTION TO THE NEXT LEVEL

So you have designed and implemented a library of analytics that identify a variety of indicators of improper payments, including P-Card, T&E expenses, and programs fraud. Where do you go from here?

For most organizations, the process of implementing fraud detection analytics is an ongoing one. Start with relatively simple tests and then add additional tests that perform more complex analysis or are intended to detect more complex types of fraud.

The majority of organizations also want to move towards a continuous process of monitoring. Once a particular form of analysis has been produced in order to detect a specific fraud indicator, it will often make sense to repeat the process on a regular basis against the most recent transactions. There are obvious advantages in detecting fraud sooner rather than later—before the extent of fraud has escalated. This often makes a good business case for analyzing and testing transactions on an ongoing basis. The actual timing of this form of continuous monitoring will vary depending on the nature of the underlying process.

TIMING IS EVERYTHING

In the case of P-Cards and T&E expenses, for example, testing is typically performed on a monthly basis, or whatever timeframe coincides with payment and reimbursement processes.

CONTINUOUS FRAUD DETECTION

From a technical perspective, the progression from using a suite of fraud specific data analysis tests on an ad hoc basis to that of continuous monitoring is not particularly complex. Assuming the issues of data access, preparation, and validation have been addressed and that the tests have been proven to be effective, then the move to continuous monitoring simply involves the regular automation of test processing.

The important issues to address are those of people and process. For example:

- Who is responsible for reviewing and following up on the results of testing?
- How often is the review and follow up to take place?
- How are unresolved items addressed?
- Who is responsible for the decision to initiate in-depth investigation and interviews?

WORKFLOW AND RED FLAGS AND DASHBOARDS, OH MY!

Software designed for continuous fraud monitoring supports this process by providing workflow capabilities. This means that exceptions indicating red flags generated by specific tests can be automatically routed to specific individuals for review. Notification of high risk exception items may be also routed to more senior management.

Continuous fraud detection software should also provide dashboards that summarize the results of analysis and test processing over a period of time. This allows senior management to review trends in the nature and amount of exceptions identified, as well as the status of items that are unresolved or under investigation. This form of reporting should ideally be integrated into an overall "data-driven" risk management dashboard supported by the information produced by continuous data analysis.

GROW YOUR FRAUD TEST BANK

In practice, organizations may establish large libraries of tests over a period of time. The fraud specialist or auditor is often in the best position to understand a specific fraud risk given the underlying business process. Analytics should ideally be developed to reflect both known risks as well as to create reports that indicate potential risks in circumstances that are not likely to be foreseen.

11 STEPS FOR TESTING FOR FRAUD, WASTE, AND ABUSE IN GOVERNMENT

The following are the basic steps that typically need to be addressed in order to create an effective and sustainable automated fraud, waste, and abuse detection process:

01. Define overall objectives, particularly in terms of whether the fraud detection process is part of an overall risk management and control testing strategy, part of a regular internal audit process or a standalone function.

02. Assign initial responsibilities for each of "people, process, and technology," both for the implementation project and ongoing.

03. Identify and define the specific fraud risks to be tested—effectively creating a "fraud risk universe."

04. For each risk, identify and define a data analysis fraud detection test in terms of:

- data requirements
- data access processes
- analysis logic

05. Coordinate with IT department (or external vendors in the case of P-Card or credit card data) as needed for issues of data access and any centralized processing requirements.

06. Develop the tests.

07. Validate the effectiveness of the tests.

08. Establish timing and responsibilities for automated test processing.

09. Establish workflow and responsibilities for exception management and resolution

10. Implement reporting processes.

11. Having started with a core set of relatively straightforward tests, progressively build and implement a broader "library" of more specific tests that address fraud risks that may be unique to your organization.

GET STARTED NOW!
BY PICKING ONE FRAUD, WASTE, OR ABUSE RISK TO TEST


SALE
SALE

CUSTOMER TESTIMONIALS

"We are embracing new technologies to better serve our mission and the public by continuously monitoring each and every transaction in order to prevent loss. We are accountable to the people of Massachusetts, and through use of ACL's technology, we are able to strengthen our risk management processes and provide more value to those who travel through the Commonwealth using our transportation system."

– Richard A. Davey, Secretary & CEO, Massachusetts Department of Transportation

"We identified a need within University Audit for a more effective and efficient process to perform and document our audit projects, and ACL's data-driven GRC technology was a great fit. The consulting services and ACL's service-oriented approach have created a smooth implementation process and served as a valuable resource throughout the purchase and implementation."

–Tracy Grunig, Director of University Audit, Arizona State University

"We were impressed by ACL GRC's flexibility, visually appealing features, and ease of use. We're really looking forward to seeing improvements in our productivity once the technology is implemented."

–Mark Petterson, Chief Audit Executive, Northern Arizona University

"ACL's solutions are the gold standard in risk and control data analysis, so it was a straightforward decision to employ its full audit management solution as part of our efforts to leverage modern technology. We now have an audit management system that effectively helps us achieve our mission of providing objective analysis and information that is critical to better decision making and enhances the overall governance capability within TDOT."

–Mel Marcella, Director of Internal Audit, Tennessee Department of Transportation

ABOUT THE AUTHOR

John Verver, CA, CISA, CMC, Vice President, Strategy, ACL, is an acknowledged thought leader, writer and speaker on continuous controls monitoring and data analytics. He is a member of the advisory board for the Continuous Auditing Research Lab and a key contributor to publications including The IIA Global Technology Audit Guide (GTAG) 3: Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment.

ABOUT ACL

ACL delivers technology solutions that are transforming audit, compliance, and risk management. Through a combination of software and expert content, ACL enables powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

Driven by a desire to expand the horizons of audit and risk management so they can deliver greater strategic business value, we develop and advocate technology that strengthens results, simplifies adoption, and improves usability. ACL's integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—combine all vital components of audit and risk, and are used seamlessly at all levels of the organization, from the C-suite to front line audit and risk professionals and the business managers they interface with. Enhanced reporting and dashboards provide transparency and business context that allows organizations to focus on what matters.

And, thanks to 25 years of experience and our consultative approach, we ensure fast, effective implementation, so customers realize concrete business results fast at low risk. Our actively engaged community of more than 14,000 customers around the globe—including 89% of the Fortune 500—tells our story best. Here are just a few. Visit us online at www.acl.com

Need Help?

To get help setting up your program to prevent fraud, waste, and abuse, call ACL at 1-866-669-4225 or email solutions@acl.com