Combatting Purchasing Card and T&E Expense Fraud:

Getting Started Guide

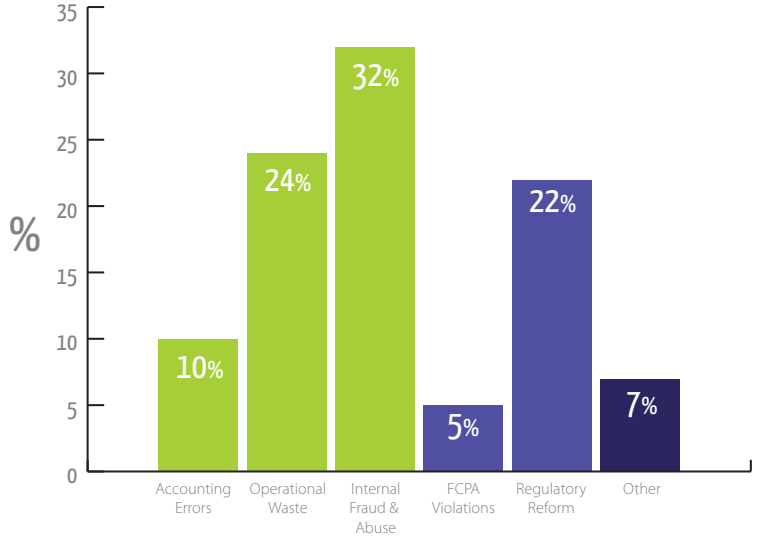
By John Verver, CA, CMC, CISA, Vice President, Product Strategy & Alliance, ACL

Combatting Purchasing Card and T&E Expense Fraud: Getting Started Guide

By John Verver, CA, CMC, CISA, Vice President, Product Strategy & Alliance, ACL

INTRODUCTION

A recent report conducted by the research arm of *The Economist* magazine found that fraud incidents grew by nine percentage points during the past year and that fraud risk is increasing. These findings align with ACL's *2013 GRC Technology Pulse Survey* of 2,200 audit, risk management, and compliance professionals, which indicated that internal fraud and abuse is an area of highest concern among a range of risks.



Largest Concerns for 2014 [1]

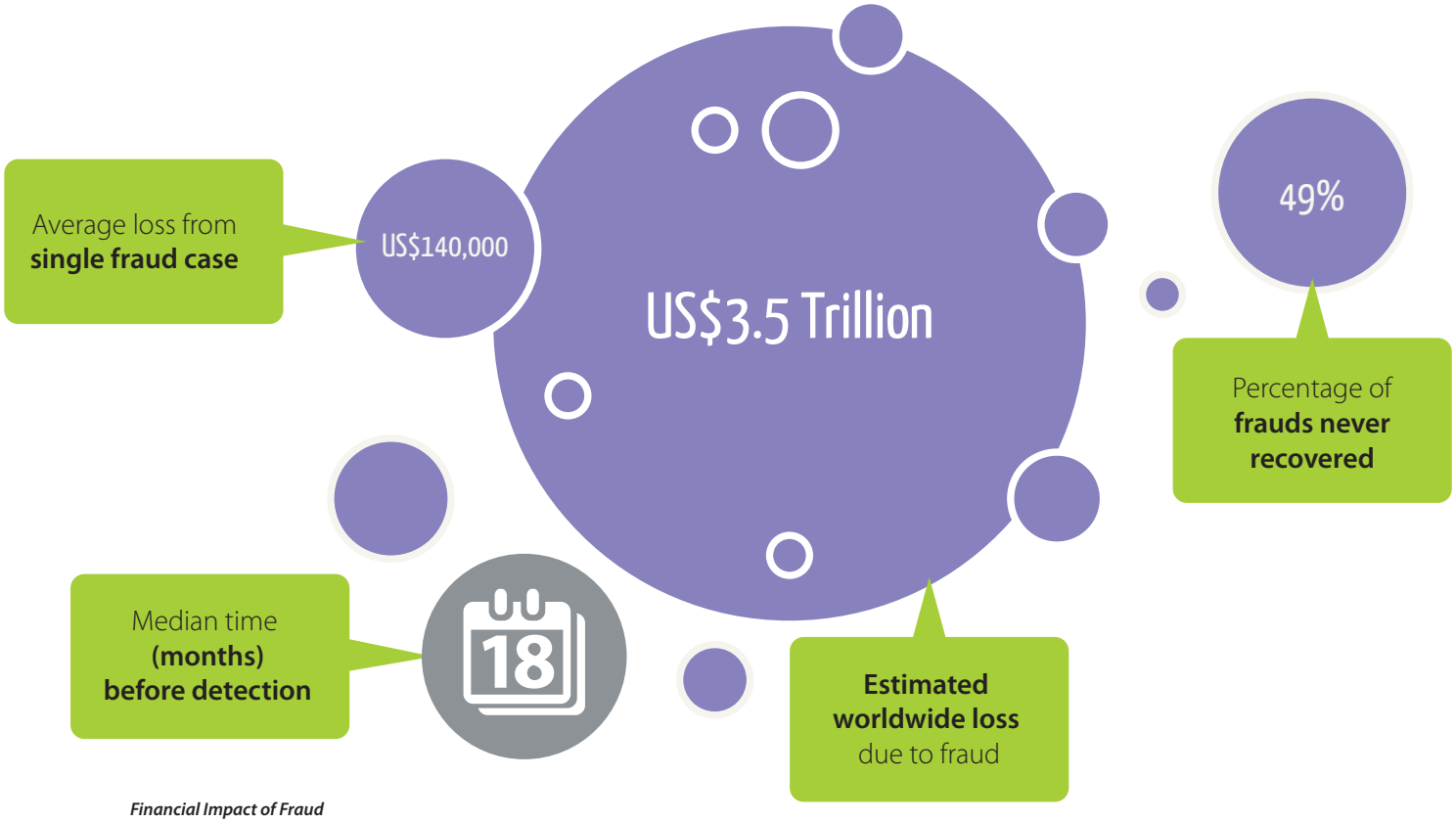
Fraudulent use of purchasing or procurement cards (P-Cards) and fraudulent claims for travel and entertainment expenses (T&E) rank among the most commonly occurring types of employee fraud.

According to the Association of Certified Fraud Examiners' (ACFE) most recent *Report to the Nations on Occupational Fraud and Abuse*, T&E frauds alone account for 14.5% of all frauds uncovered. If there is a risk that T&E or P-Card fraud becomes widespread within an organization, it is easy to see that total losses can represent a significant sum. Of course, the negative impacts on an organization resulting from these forms of employee fraud are not limited to monetary ones. In organizations where such fraud does become widespread, it is often symptomatic of a general unethical attitude: "I know others are doing it—why shouldn't I?"

So, what to do about it?

Although instances of P-Card and T&E fraud are commonplace, they are both areas that are relatively easy to address. Most organizations start by ensuring that there is an appropriate tone at the top, clearly defined ethical policies and well-designed controls. These are, of course, the right places to start when implementing any program designed to address employee fraud.

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



Financial Impact of Fraud

> "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.

P-Card and T&E are both areas in which the use of technology, specifically data analysis technology, has a critical role to play inidentifying 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.

HOW IS DATA ANALYSIS ACTUALLY USED TO DETECT PURCHASING CARD AND T&E FRAUD?

There are two primary ways in which data analysis is generally used to detect a broad range of types of fraud, including P-Card and T&E fraud.

01. **The first is to analyze entire populations of transactional data to look for various forms of anomalies**. This often includes data from a wide range of systems, including third parties such as credit card vendors and expense card management systems such as Concur. Transactional data analysis does not necessarily prove that fraud has 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, would one employee with the same job responsibilities as a hundred others claim 50% more travel expenses? There could be several valid reasons why this could be justified. But if no reasons are obvious, then it could be a valid indicator of increased risk of fraud having occurred.
02. **The second and more specific approach is to analyze transactions for indicators of known fraud risks.** An employee may be authorized, for example, to use a P-Card for purchases of specific business items. If an analysis of P-Card data shows that a purchase was made from a consumer products store, this could be a strong indication of an actual fraud.

The (in)dispensable spreadsheet

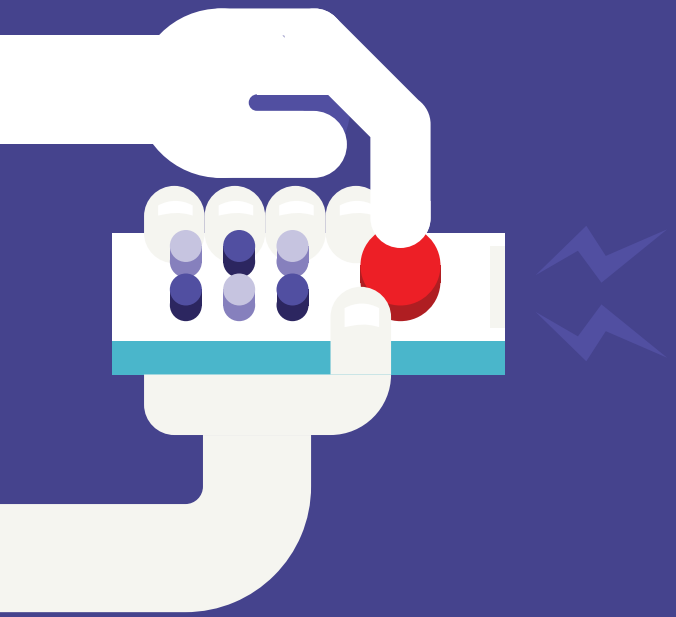
For those involved in fraud detection, the ease-of-use, adaptability, and low cost of spreadsheets may make it a strong draw. Beware. Organizations need to balance the appeal of spreadsheets against their shortcomings, including:

- **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 overreliance 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. A simple example in the case of P-Card or T&E is to compare payment information with HR records to see if there are instances in which an employee has been using a P-Card or claiming expenses while on vacation.

Another example is to compare employee descriptions of expenses with the data available from credit card companies on merchant codes and expense categories. What an employee describes as the cost of a training course or business publication subscription may turn out to be an expense incurred on an online gambling site (or, in one case we heard about, on the site of an online psychic!).

Other types of data analysis involve testing to see if ERP application control settings, or master file data, have been changed in a way that indicates potential fraud. What if a manager was authorized to approve P-Card items 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?

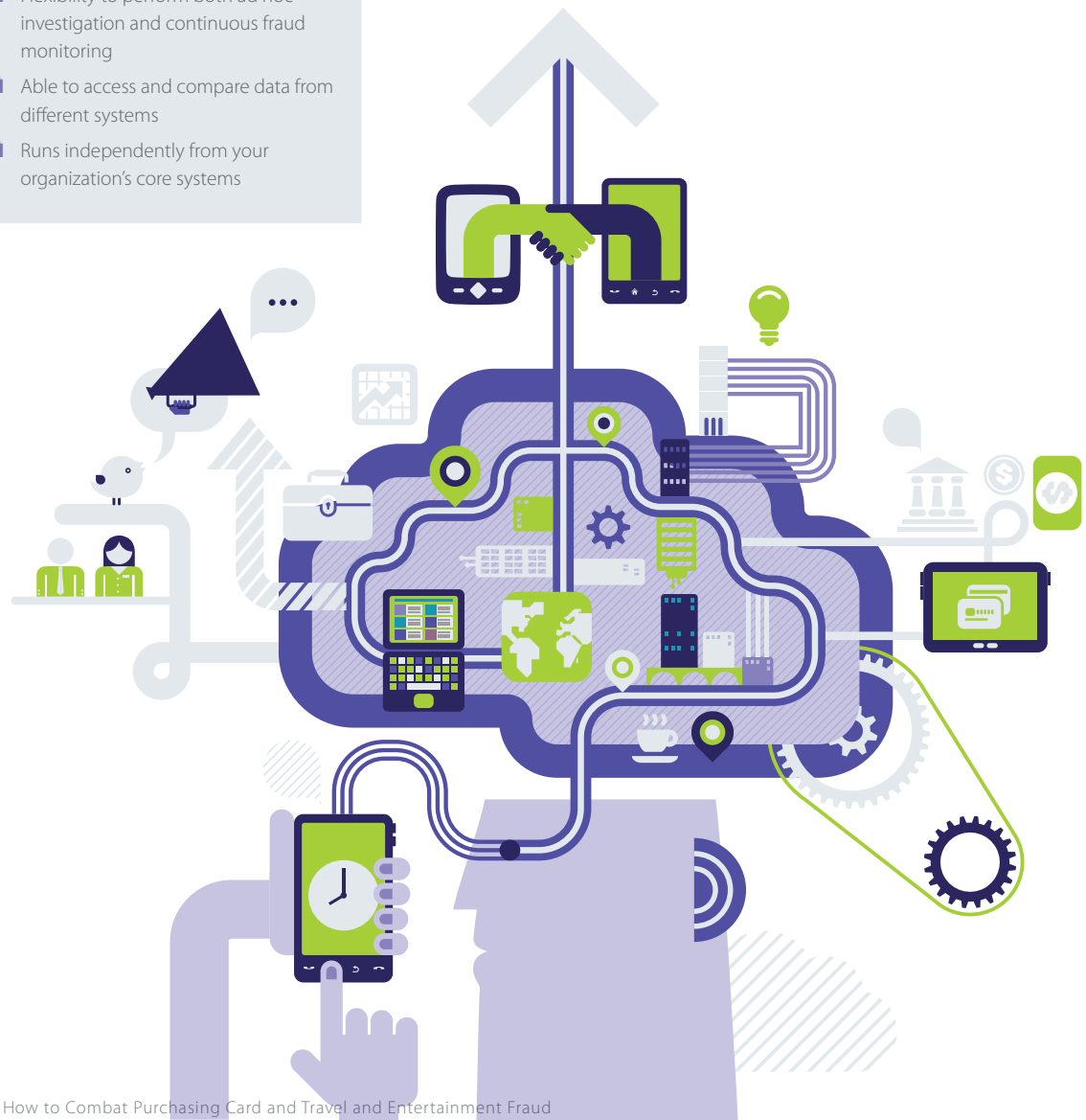
TO SAMPLE OR NOT TO SAMPLE?

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: DATA ANALYSIS FOR FRAUD DETECTION



Data analysis software designed specifically for fraud detection has specific functional capabilities. In general, these capabilities are similar to those for data analysis in audit or for other 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. Software for fraud detection 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 important capabilities of data analysis technologies for 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 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 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:

P-Card

HOW TO IDENTIFY EMPLOYEES' FRAUDULENT USE OF PURCHASING CARDS

Purchasing cards (P-Cards) are increasingly used by businesses and 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 credit 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

- A large international bank immediately identified a single expense fraud with an exposure of US$30,000 and identified 244 occurrences of abuse in corporate late night expenses in a single month.
- 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 organizations in which employees are provided with corporate 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 T&E expenses.

T&E expenses represent a significant percentage of overall expenditures for many organizations. It is an area particularly prone to a sense of entitlement by some employees. This may be based on the old traditional practice of providing "expense accounts" to certain categories of employees. Most organizations have moved to formal policies for allowable T&E claims, but instances of abuse can be commonplace.

In some organizations, the biggest concerns arise in the practices of more senior management. Not only can the monetary amounts involved be substantial, but also there can be significant damage to a corporate brand if it becomes known that T&E abuse is taking place at a high level.

TRAVEL & ENTERTAINMENT FRAUD TESTS

T&E

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

TAKING FRAUD DETECTION TO THE NEXT LEVEL

So, you have designed and implemented a library of analytics that identify a variety of indicators of P-Card or T&E 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, testing is typically performed on a monthly basis, or whatever timeframe coincides with payment and reimbursement processes.

An ounce of prevention is worth a pound of cure

Being able to detect P-Card or T&E fraud when it occurs is clearly valuable. The sooner a fraud is found the sooner the risk can be addressed—before it has the chance to escalate into something that causes greater damage. Of course, the adage "an ounce of prevention is worth a pound of cure" makes sense in that it avoids the problem in the first place. The challenge is how to achieve this. No control system is perfect. In fact it would become very inefficient if controls become so pervasive that they get in the way of operational efficiency and good business sense.

One of the benefits of using transactional monitoring to look for fraud is that it can become part of the control process itself. There is often value in clearly communicating that monitoring is taking place—as part of a broader organizational communication about zero tolerance to fraud. If employees and management are aware that monitoring is taking place—specifically intended to identify abuse of P-Cards and T&E claims—then the chances are that individuals who may have been tempted to "get away" with something will think again.

CONTINUOUS FRAUD DETECTION

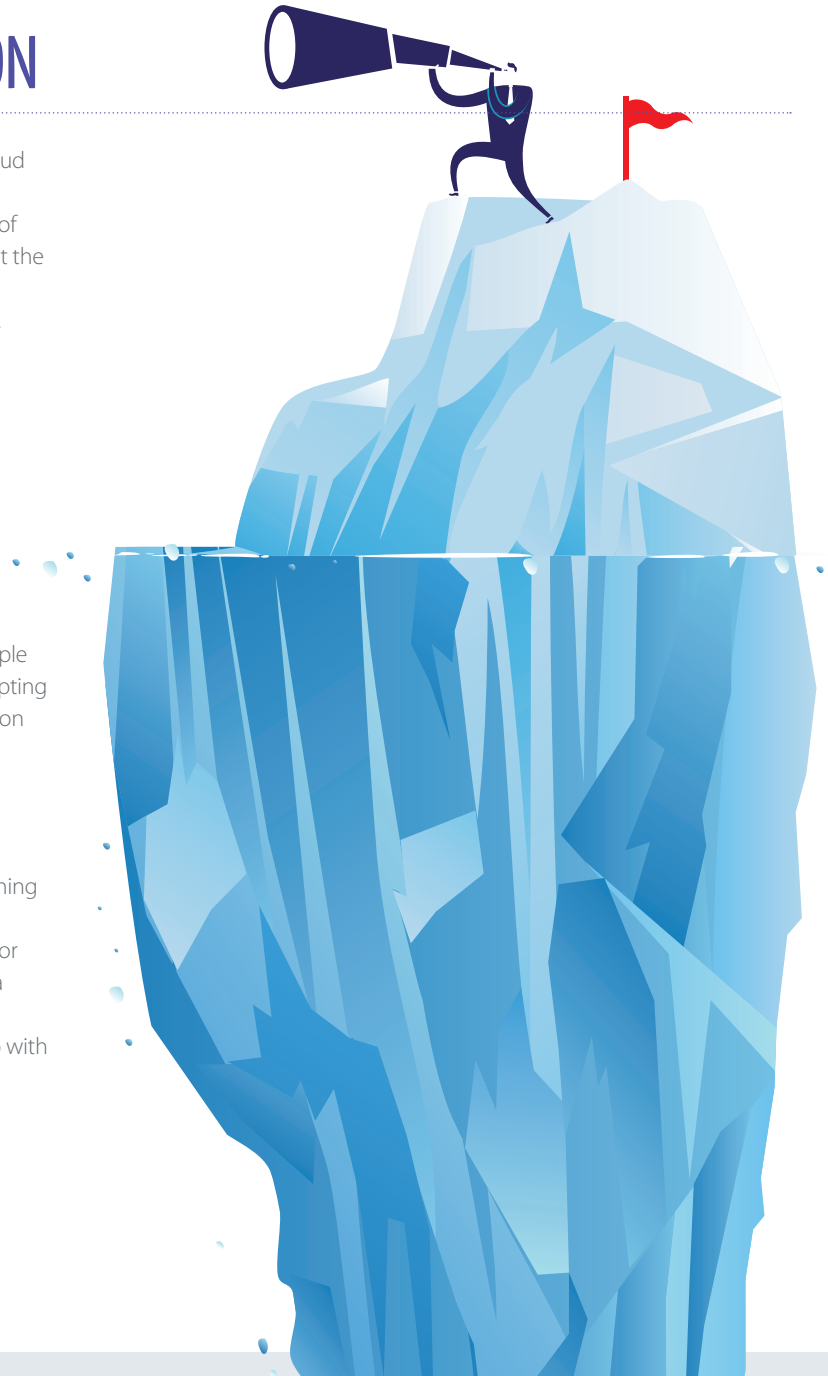
From a technical perspective, the progression from using a suite of fraud specific data analysis tests on an ad hoc basis to that of continuously monitoring for fraud is not particularly complex. Assuming the issues of data access, preparation, and validation have been addressed and that the tests have been proven to be effective, 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?

Once everything is in place to monitor transactions and all of the people and process activities are working on an ongoing basis it may be tempting to think that the job is done. In practice, fraud monitoring and detection needs to be a dynamic process. As with most types of risks that an organization faces, they are rarely static. Systems change, business processes change, and those tempted to commit fraud will always be thinking of new ways to "beat the system."

Data analysis has a valuable role to play in this area. In addition to running a suite of specific fraud detection tests, it is important to also use data analysis to regularly profile entire populations of transactions to look for things that just do not seem to make sense or look right. This can be a good way to identify types of fraudulent activity for which no consideration had previously been given. Data analysis can really help with the things that "you don't know you don't know."



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 P-CARD AND T&E FRAUD

The following are the basic steps that typically need to be addressed in order to create an effective and sustainable automated fraud 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 RISK TO TEST


SALE
SALE

ABOUT THE AUTHOR

John Verver, CA, CISA, CMC, Vice President, Product Strategy & Alliances, 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 T&E and P-Card Fraud Detection Program, call ACL at 1-866-669-4225 or email solutions@acl.com