

Leveraging the Economics of Corporate Credit Cards

The role of continuous fraud analytics
in the distributed buying model

Oversight ™
Find it. Fix it. Prove it.

The use of corporate credit cards is on the rise, for everything from office supplies, to temporary employment services, to fuel, telecommunications and travel expenses. According to RPMG Research Corporation's *2006 Corporate Travel Card Benchmark Survey Results*, corporate travel card spending increased from \$120 billion in 2004 to \$143 billion in 2006, and growth is expected to continue to \$227 billion in 2010. The same study shows that from 2003 to 2005, there was more than a 35 percent increase in corporate procurement card spending. This represents a compound annual growth rate of 12.3%, and that level of growth is also expected to continue through 2010.

Corporate cards deliver tremendous economic benefit to companies, in terms of expanded buying power and ease of use – not to mention card-issuer incentives. Again, RPMG reports that corporate card purchases represent minimal transaction processing expense; with an estimated average transactional cost of traditional procurement running from \$50 to \$250, procurement cards can result in corporate savings of 55% to 90%. But along with this distributed buying power come challenges, such as ensuring adherence to purchasing and expense policies, as well as detecting misuse and fraud. Studies show that the impact of such violations is higher than average transaction value. Individual violations can be small, but the total can be significant.

Corporate card violations are usually indicative of violations elsewhere, and cash reimbursements, as in the case of travel and entertainment (T&E) expenses, leave the door wide open for abuse. As a result, many companies are beginning to employ continuous monitoring, or continuous fraud analytics, as a method for overcoming these challenges so that they can safely expand the use of corporate cards to maximize program value.

Configuration of corporate card fraud analytics

Corporations with high-volume corporate card programs have found that eliminating fraud and policy violations within the distributed buying model relies on two key elements: a cross-system view of enterprise data; and the ability to analyze every corporate card transaction, in near real-time.

Cross-system enterprise data view

A cross-system view of non card-specific enterprise data is required due to the nature of corporate card usage. In the case of travel and entertainment (T&E) expenses, the transactional data available from the card provider is only one component of the expense transaction profile. Equally critical to effective fraud analysis and policy enforcement are data from the expense management system, if one is in use, as well as data on the card user, from the perspective of the Human Resources (HR) system.

For example, only the cross-system view will flag as suspicious a “spending spree” that takes place on the last effective date of employment of a terminated employee. While the actual charges to the card are, on their own, perfectly legitimate from the card-provider perspective, the broader circumstances of the card use is suspect in terms of its inherent business value to the corporation, and may actually constitute a clear violation of company expense policy. In another example, data from the expense tracking system analyzed in conjunction with the transactional data from the card provider will reveal expenses charged directly to the company through use of the corporate credit card, that are also submitted by the employee for reimbursement on an expense report – thereby creating a duplicate payment condition.

Corporate credit cards used for procurement offer significant economic advantages to the company, in terms of leveraging volume discounts, distributing purchasing approvals and

processing, and streamlining operations. Procurement cards have the same issues as travel cards in terms of fraud analytics, requiring card transactional data to be analyzed in conjunction with Accounts Payable (AP) data, as well as HR records. As with the previous examples, the HR data will reveal procurements by employees while on suspension, or out of their area of purchase authority. AP data will flag purchases charged to the card for which there is also an invoice from the vendor, representing a duplicate purchase, or resulting in duplicate payment for a single purchase.

Analyze all card transactions in near real-time

The second element to successfully eliminating fraud and misuse in corporate card programs is the ability to analyze every corporate card transaction, in near real-time. In a low-volume environment, in terms of the number of employee card holders and/or the number of transactions, it may be possible to make a financial case for manual oversight. But as these programs scale – as they must, to deliver maximum value to the corporation – such manual analysis becomes impractical or impossible.

At this point, some program managers will institute a “sampling” based approach to auditing corporate card transactions. They may set up schemes such as auditing a set percentage of transactions or card holders each month, auditing a specific card holder X times each year, auditing new card holders for the first few months, or auditing arbitrary groups of card holders’ transactions on a rotating basis. These organizations are typically happy to audit 25 to 35 percent of their total card transactions, but often there is no rigor in determining the potential economic impact of leaving the remainder unchecked.

Because the typical violation includes a pattern of repeated activity, the danger inherent in this kind of “control” environment is best reflected in the following comment from

the program manager for a Fortune 200 company with thousands of card holders and more than a million transactions to audit: "By not having a way of auditing 100 percent of card transactions, and enforcing policies consistently across the organization, you run the risk of inadvertently allowing a culture of entitlement to grow up around inappropriate use of the card. There is a perceived statute of limitations; card holders may think, 'They haven't stopped me for years; I've always done it this way.'" In fact, the RPMG study showed that 1 out of every 5,000 transactions is questionable (at best); in this company, that statistic played out in the form of over 250 policy violations worth nearly \$1 million found within the first six months of implementing a continuous fraud analytics solution.

The economics of policy enforcement

Putting corporate buying power into the hands of employees, in essence, making each employee an authorized purchasing agent of the company, significantly increases the importance of establishing strong usage policies and restrictions. Here, as in the area of fraud detection, companies need a continuous analytics mechanism that can look beyond the limitations that can be enforced and reported by the card provider. Some policies regarding the use of the corporate card can be enforced by the card provider. For example, in order to enforce policies regarding the nature of purchase, the card provider can restrict purchases at the Merchant Category Code (MCC) level, such as precluding the use of the card for purchases from department stores. Problems can arise with this restriction in a couple of ways. For one thing, merchants self-identify their MCC, so a merchant can appear to be in a valid category, while still offering a high percentage of merchandise that is not allowed under company purchasing policies. In addition, because categories are broad, the MCC could actually exclude a valid merchant – even one with whom the company has negotiated significant corporate discounts. The

granularity of control offered by sophisticated continuous fraud analytics allows the company to open up categories, while still maintaining control.

The value of this focused policy enforcement is evidenced in the company whose program manager was quoted earlier. The company had made an arrangement for special pricing with a particular airline out of Chicago, and their expense policy required that company travel from Chicago be booked exclusively on this airline. However, given the limitations of MCC restrictions, the card provider won't stop the employee card holder from purchasing tickets from different airline, thus costing the company through the loss of their negotiated discounts.

The real economic issues of fraud prevention and policy enforcement become clear when you look at the business structure of the principal gatekeepers – the card providers. Their primary customers are the merchants, who represent income to the card provider that typically ranges from five to seven percent of each transaction charged to the card. Clearly, their main objective is to maximize – not control – the number and dollar amounts of corporate card transactions. Although they do sell reporting and analytical tools to corporate card users, these are rudimentary, limited by the card providers own limitations on analytical data, and do not constitute a proactive notification of exceptions. Using these in a high-volume environment can't begin to approach the near real-time analysis required for finding and dealing with fraud, misuse and policy violations early in the process, where they are easier and less costly to address, and where the enforcement value is much higher.

(cont. on next page)

Continuous fraud analytics

Continuous fraud analytics for auditing corporate credit card transactions are based on continuous transaction monitoring (CTM) technology. This is a category of software that can extract data from multiple sources: the company's internal financial systems, such as AP and HR systems; third-party applications, such as expense management applications; and transaction data from the corporate card provider. The software extracts and maps the data into a common data model, then applies sophisticated analytics to precisely identify transactions which might constitute policy violations, fraud, or misuse. The transactions are tested against pre-defined integrity checks that are based on the company's policies and best practices. Examples of such integrity checks might be:

- Approved merchants not used

- Potential policy violations (name on airline ticket does not match cardholder name; use of luxury hotels)

- Inactive employee (on leave of absence; terminated)

- Merchant suspicious (department store, online, jewelry, apparel, cruise)

- Amount suspicious (\$ amount, denomination, high retail price)

The more near-human reasoning is incorporated into the CTM analytics, the more effective they will be in precisely identifying problems, for example, identifying "unusual", "similar", or "usual" transactions. This may be based on structural and knowledge-based approaches, such as identifying when critical fields are malformed or missing, surfacing apparent duplications, and flagging second-order anomalies (e.g. negotiated rates compared to amount expensed).

Statistical approaches serve to flag numerical and discrete valued outliers, timing and frequency anomalies, and combinations of above. Similarity comparisons find items such as account number 123456 resembles 1230456. Temporal reasoning tracks transaction relationships thru time, for example, identifying recurrence that is part of a pattern which may indicate fraudulent purchase or expense transactions. It is this kind of sophisticated investigative reasoning that keeps companies holding on to manual auditing long after they have reached a transaction volume that precludes its effectiveness. Program managers should look into current CTM technologies, which automate this type of artificial-intelligence based analysis to provide both the accuracy and the scalability needed in high-volume environments.

Setting the tone at the top

One of the most financially beneficial aspects of implementing continuous fraud analytics to monitor corporate card transactions is the deterrent effect. Not only does the knowledge that there is an automated investigation of every transaction serve to make employees less likely to violate company policy or use the card fraudulently, it also sets a tone at the top: violations will not be tolerated. This goes a long way toward eliminating that “culture of entitlement” – so long as management is willing to act on the results of the analysis.

There is no reason for today’s companies to miss out on the benefits of the distributed buying model, nor is there any reason for them to suffer the offsetting losses created by unchecked misuse. The key is to understand the limitations of the card provider in controlling fraud and policy violations, and to take advantage of continuous transaction monitoring technologies that incorporate a cross-system view of enterprise data and automate the analysis of every corporate card transaction, in near real-time.