

Fraud Resistant P-cards

DONALD HOLDEGRAVER

DIRECTOR-OPERATIONS ANALYSIS
UNIVERSITY OF NEBRASKA-LINCOLN

Procurement card programs can't be foolproof, but there is help.

PROCUREMENT CARD (P-CARD) USE HAS INCREASED dramatically since the mid-1990s when the cards were first introduced on a wide scale. Served by a growing number of providers worldwide, p-cards can be a source of organizational efficiency and effectiveness by reducing purchasing costs, especially for small-dollar items. P-card purchases have doubled in recent years, according to published statistics, and the expectation is that this growth will continue into the foreseeable future as organizations add cardholders, increase limits, and expand categories of purchases eligible for p-card use. P-card programs can also be a source of revenue, as providers vie for the growing p-card market through increased incentives and revenue returns.

Policies and procedures are the heart of a fraud-resistant p-card program, but they must do more than list prohibited uses and who to call if the card is lost.

Unfortunately, where there's money, there's the potential for fraud, and p-cards are no exception. As organizations have expanded their p-card use, they have allowed a growing number of employees to purchase from a growing number of vendors, with higher per-transaction and period limits, and often less control and monitoring over the transactions. Combining the ability to use p-cards at a variety of vendors with being relatively unobserved by co-workers, the result can be a p-card program in which fraud is occurring despite what appears on the surface to be a well-controlled program.

In 1995, the University of Nebraska-Lincoln (UNL) launched a pilot p-card program with fewer than 50 cards spread over four departments, each card with a single transaction limit of US \$499. For the next eight years, cardholders were encouraged to expand their use of the cards as a cost-saving measure so that by 2003, the program had grown to more than 1,200 cards with a single-purchase limit of US \$1,499 and usage totalling 70,000 transactions and nearly US \$12 million. Specific responsibility for monitoring transactions was vested in the management teams of the departments to which cards were assigned. In addition, only one individual in the accounting department was assigned responsibility for reviewing each p-card transaction for obvious signs of abuse or fraud. As the program grew, the risk grew as well.

Until 2001, only limited efforts were made to independently assure that department management was monitoring p-card use correctly. Sporadic audits of p-card use were completed by UNL's internal audit department, Operations

Analysis. In 2002, at the request of a short-staffed accounting department concerned about its ability to monitor for potential fraud and abuse in the program and follow state transaction pre-audit rules, Operations Analysis expanded its p-card audit program by scheduling quarterly reviews of selected departments' use. The expansion of the audit process culminated in 2003 with the discovery of a p-card fraud that had been ongoing for three years in one small operating unit of the university and resulted in a loss of more than US \$30,000.

Fraud in p-card programs can take many forms. It can be as simple as a cardholder buying a personal item with the intent of having the university pay the bill. But p-card fraud is insidious because even fraudulent users can appear to be making legitimate purchases based on job duties, but actually may be making unauthorized buys, such as:

- Facilities maintenance staff buying paint, wall coverings, tools, and other maintenance related items for part-time, non-business related, personal handyman businesses.
- Information systems staff purchasing excessive quantities of peripherals and electronic components for repairs and upgrades to friends' and family members' personal computers, or outright sale to unsuspecting customers of part-time computer businesses.
- Mixed purchases (i.e., business and personal items on one purchase receipt) at discount stores that are fully charged to the organization because of inadequate after-the-fact monitoring.
- Purchases of materials and services that, under any other purchasing process, would have been questioned before the transaction was completed, but ease of

use of the p-card allowed unsupervised purchases.

Dr. Steve Albrecht, associate dean—Marriott School, Brigham Young University, commented in a seminar for the Association of Certified Fraud Examiners' Heartland Chapter in Omaha, Neb., that, "When you have a fraud, you don't have a fraud problem; you have a business problem." With procurement cards, this is certainly true. The fraud experience at UNL prompted a detailed review of the p-card program, and the launch in 2004 of a new and improved p-card program that was designed to be fraud resistant while still maximizing the benefits of p-card use to the university.

Although it is good business to mitigate as many fraud risks as possible, organizations must understand that a p-card program, no matter how well designed, cannot be assured to be fraud-free. However, using 12 basic steps, organizations can make their p-card programs more fraud resistant while maximizing the ability of employees to use p-cards to purchase efficiently at the lowest possible cost.

1. Design dedicated and detailed policies and procedures and update them regularly to reflect the p-card program roles and responsibilities accurately.

Policies and procedures are the heart of a fraud-resistant p-card program, but they must do more than list prohibited uses and who to call if the card is lost. As with any operating activity, well-designed policies and procedures spell out the accountabilities and responsibilities of cardholders and those responsible for monitoring card usage. Unless the who, what, where, when, and how of p-card use, monitoring, and control are specified, fraud will happen. Although policies and procedures alone won't prevent fraud, they are the foundation on which a fraud-resistant program is built.

2. Appoint a permanent administrator with responsibility for, and authority over, the p-card program.

A p-card program cannot be fraud resistant without a dedicated administrator who assures that cardholders are trained and card usage is monitored. The most effective p-card program tool I ever witnessed was the card services manager who

brought a long, gold-handled pair of shears to each training session. It went almost without saying what would happen to the cards of those who misused their responsibilities for their assigned p-card. A dedicated administrator for the p-card program also will assure that all aspects of the card program are kept up to date and reflect the most current technology and management controls available.

Administrators should be responsible for card distribution, training — and retraining — cardholders and transaction reconcilers, and monitoring for incidences of possible unintentional personal use or obvious misuse. They should also be responsible for approving officials who provide the daily oversight for the program, assuring that the contract terms are fulfilled by both the organization and the card providers, and regularly reviewing p-card provider services, rebidding the contract when appropriate.

3. Implement a detailed cardholder agreement requiring the signature of the cardholder and the cardholder's supervisor to reinforce responsibility and to improve accountability.

Although the primary responsibility for using the card in accordance with policies and procedures rests with the cardholder, the supervisor has the ultimate accountability for how the card is used. By having the supervisor sign the agreement, he or she is reminded that the ultimate accountability for each purchase the cardholder makes rests with the supervisor, and the supervisor accepts a monitoring role over the cardholder's card use. Each level of monitoring instituted in the p-card program is one more way to minimize potential p-card misuse and abuse.

4. Designate and communicate detailed roles and responsibilities for the transaction reconcilers and approving officials.

A primary error made in p-card programs is to have a subordinate to the cardholder reconciling or approving card transactions. At UNL, separate individuals are assigned as reconciler — responsible for gathering the supporting documents and posting the transaction to the financial system — and

approving official — responsible for signing off before or after each purchase. The individuals who reconcile and approve transactions should not be under the direct supervision of the cardholder, and should be able to make independent judgments about the appropriate use of the card. Documented, specific responsibilities for each person involved in the card-use and monitoring process will assure that all transactions get an appropriate level of scrutiny and approval, and that responsibility will be segregated appropriately.

5. Use a p-card design that minimizes the possibility of "accidental" use.

The second most common violation of p-card rules at UNL, and doubtlessly at many other institutions, has been, "I accidentally used my p-card for a personal purchase when I was in a hurry." Even assuming that most such "accidents" are truly mistakes, the p-cards can be designed to minimize this response when an intentional personal purchase is suspected. At UNL, the new card is a bright aqua color with *University of Nebraska* and *Purchasing* embossed in large lettering on the face of the card, enclosed in a sleeve to protect the card and remind the cardholder that it's for business use only. The design and packaging makes "accidental" use virtually impossible.

6. Establish reasonable card limits to reduce excessive or inappropriate use issues.

Programs often start out with low transaction limits, but purchasing directors quickly realize that they can reduce purchasing costs and increase incentive

revenues by increasing card limits to the highest level possible. This has caused organizations to establish limits far above the necessary levels. In one well-publicized U.S. federal agency case in 2002, an individual from Los Alamos National Laboratory who had a high five-figure p-card limit was accused of trying to negotiate the purchase of a Ford Mustang on his card. In other publicized instances, individuals used federal government p-cards for large personal or luxury purchases, and even cosmetic surgery.

A good rule to follow is to provide card limits that slightly exceed the highest actual purchase in the preceding year by a cardholder. Limits should be defined by employee, or by employee class or use, not by establishing blanket limits for all cards. Blanket limits give some individuals considerably more purchasing power than they will ever need or use, which increases the risk of abuse and the impact to the organization should the card be misused.

7. Require face-to-face training before issuing a p-card to a new cardholder, and require refresher training at least every two years for continuing cardholders. The refresher training can be face-to-face or computer/Web-based.

In real estate, the guiding mantra is "location, location, location." In p-card programs, it's "training, training, training." Face-to-face training should be required for every new cardholder, followed by an annual or biannual refresher course. Face-to-face training assures that the appropriate emphasis can be applied in the initial training, and it allows new cardholders to ask questions. Most cardholders will use the cards properly if they receive the necessary instruction in the

A purchase should never be reconciled or approved without detailed supporting documentation that delineates the entire amount charged, as well as the specific business purpose of the purchase.

Although routine monitoring processes are best handled by each operating unit's management, regular surprise audits of card usage, combined with data mining and analysis of usage anomalies and transaction information, provide a one-two punch of oversight that can deter fraud significantly.

beginning. Use of computer-based or Web-based training is an option, but should be used only after initial face-to-face training.

8. Require original receipts for every p-card purchase made.

Every photocopy accepted in support of a p-card transaction is an increased risk of fraud or abuse. In the electronic age, it is more difficult to obtain original vendor documentation, but it should still be emphasized. In the absence of original vendor documents, every document available to support the transaction should be required. With today's Internet purchases, a printout of a detailed order form is often the only original document initially provided. Cardholders should be required to include the order confirmation screen and, if received, the order confirmation e-mail to support Web purchases. These should be in addition to any receiving document or packing slips included with the delivered purchase.

A purchase should never be reconciled or approved without detailed supporting documentation that delineates the entire amount charged, as well as the specific business purpose of the purchase. The specific business purpose might include the contract, agreement, project number, grant, or other specific reference to identify how the purchase was used, to assure the purchase can be accounted for and tracked appropriately.

9. Require electronic transfer of cumulative data from the card-services provider for data mining and analysis based on known risk factors.

The development of comprehensive software to analyze databases for transaction

anomalies has increased the importance of access to electronic data, and it has improved monitoring of all types of transactions. Using software to identify anomalies such as split transactions — multiple transactions designed to circumvent card limits — over-limit purchases, unusual transaction patterns, use of non-standard vendors for standard purchases, and even-dollar transactions at or just below threshold levels will allow more efficient and effective monitoring and prevention or detection of potential misuse situations. Defining these anomalies is key to electronic data analysis of p-card activity.

Assuring that the card service provider has the ability to produce Level 1, 2, and 3 transaction information is critical to this analysis process. This information breaks each transaction down by MCC code, type of service, vendor identification, and vendor corporate status to assure operational, financial, and tax-related information is available to the organization for analysis and use.

10. Provide a hotline process to report suspected abuse.

It is safe to say that in virtually every p-card fraud, at least one other person knew about or suspected the fraud, but didn't know how to report his or her knowledge or suspicion. At UNL, the lack of a defined process to report suspected fraud was a contributing factor to the fraud. Providing a confidential way for individuals to report suspected p-card fraud and abuse, and publicizing the process through training and ongoing communication from the p-card administrator, will strengthen a p-card program exponentially.

11. Have meaningful and enforced policies governing consequences for misuse.

Consequences for misuse must be real, known, and enforced. Any misuse of a p-card should be treated as a violation, and proven use of a p-card for personal purchases should be considered an act of theft. The fraudster should be prosecuted, and the prosecution should be publicized. Not prosecuting and publicizing thefts and their consequences reinforces an "anything goes" mind-set that will result in more fraud. The likelihood of discovery and punishment for theft is a significant fraud deterrent.

12. Institute recurring audit processes to evaluate compliance with program policies and requirements.

Although routine monitoring processes are best handled by each operating unit's management, regular surprise audits of card usage, combined with data mining and analysis of usage anomalies and transaction information, provide a one-two punch of oversight that can deter fraud significantly.

At UNL, a fraud was discovered during a routine surprise audit of the unit's p-card documentation that disclosed irregularities in the explanations for non-standard transactions and documentation. Without the audit process, the fraud may have continued indefinitely. If the p-card program generates sufficient revenue in incentives, this audit activity can be part of the card administrator's staff, funded by the incentive funds.

WRAP IT UP

P-card programs are a valuable business tool available to organizations to improve purchasing effectiveness and minimize purchasing costs. To maximize the benefits, they can be individually tailored to organizations. However, if p-card programs are not designed to be fraud resistant, they can also be a source of loss and public embarrassment. By implementing the 12 steps outlined here, p-card programs can achieve an improved level of control and monitoring that can minimize the potential for fraud and monetary loss.

To comment on this article, e-mail the author at dholdegraver@theiia.org.