Fraud Prevention and Detection: Establishing and Maintaining a Purchasing Card Program with Adequate Management Controls to Prevent Fraud, Misuse and Abuse

Edition 2.3, June 2017

Advancing Commercial Card and Payment Practices Worldwide
Terms of Use

This content is protected by copyrights owned or licensed by the NAPCP. You may not reproduce, perform, create derivative works from, republish, upload, post, transmit or distribute in any way whatsoever any part of this content without the prior written permission of the NAPCP. Submit any such requests to napcp@napcp.org. However, you may download or make one copy of the materials for personal, non-commercial use only, provided all copyright and other notices contained in the materials are left intact. Any modification of the materials, or any portion thereof, or use of the materials for any other purpose constitutes an infringement of the NAPCP’s copyrights and other proprietary rights. Use of these materials on any other website or other networked computer environment without prior written permission from the NAPCP is prohibited.
Table of Contents

Acknowledgements................................................................................................................. 4
Overview .................................................................................................................................... 4
Distinguishing Between Fraud and Misuse .............................................................................. 4
Integrating Deterrents in Program Design ............................................................................. 5
Prevention .................................................................................................................................. 5
Establishing Roles and Responsibilities .............................................................................. 6
  Program Management Team .................................................................................................. 6
  Cardholders ............................................................................................................................ 6
  Approvers .............................................................................................................................. 6
  Card Issuer ............................................................................................................................. 6
  Suppliers ................................................................................................................................ 6
Ensuring Separation of Duties ................................................................................................. 7
Implementing Appropriate Policies ......................................................................................... 7
Documenting Clear Procedures ............................................................................................... 8
  Procedures for Program Participants ................................................................................... 8
  Procedures for the Program Management Team ................................................................. 9
Utilizing Systemic Controls ..................................................................................................... 10
Detection .................................................................................................................................. 11
  Auditing ................................................................................................................................. 11
  Approvals .............................................................................................................................. 12
  Documentation ....................................................................................................................... 12
  Expense Control ................................................................................................................... 12
  Reviewing, Reconciling and Approving .............................................................................. 13
Creating and Analyzing Reports ............................................................................................ 13
  Declined Transactions .......................................................................................................... 13
  Activity Analysis .................................................................................................................. 13
  Disputed Charges ................................................................................................................ 13
  Account Listing ..................................................................................................................... 14
  New Account Activity .......................................................................................................... 14
Conducting a Risk Analysis ...................................................................................................... 14
Conclusion .................................................................................................................................. 14
Additional NAPCP Resources ................................................................................................. 15
About the NAPCP ..................................................................................................................... 15
Acknowledgements

The original Fraud Prevention and Detection report was published by the NAPCP in 2004. The contributors included the following individuals, who were part of the NAPCP Best Practices Task Force at that time: Tamara Corbin, Tony Giarnella, Anne Hawley, Alex Julewitz, Cynthia Martin, Eddie Page, Julia Stout, Wanda Waite, Terri Westmoreland and Tom Wissel.

Subsequent editions (2010, 2012, 2014 and 2017) were updated by NAPCP staff to reflect changes in the Commercial Card industry.

Overview

Media reports of fraud related to the use of Commercial Cards (e.g., Purchasing Cards, Corporate Cards, etc.), particularly in publicly funded organizations, tend to receive notable attention, while rarely does the general media cover the benefits of card payments. Publicity associated with fraudulent incidents could lead one to the conclusion that such crime is significant within card programs. In actuality, industry research—on Purchasing Cards (P-Cards) in particular—has revealed otherwise, repeatedly demonstrating that fraud/misuse is not the epidemic problem that some people, especially those lacking an understanding of P-Cards, believe it to be. A large proportion of the fraud/misuse tends to occur in a small percentage of end-user organizations. Nevertheless, real or perceived laxity of controls within a P-Card program can result in withdrawal of management support and the diversion of procure-to-pay activity to alternate means.

In comparison to a traditional procure-to-pay process (e.g., one based on a requisition, purchase order and invoice paid by accounts payable), the typical P-Card process allows a business unit/department to both initiate and pay for a purchase, resulting in the need for different types of controls. This report, describing several types of controls, is designed as a resource for end-user organizations interested in minimizing the potential for P-Card fraud and misuse.

Distinguishing Between Fraud and Misuse

The terms “fraud” and “misuse” are often used interchangeably, but a distinction should be made between them:

- Fraud involves the unauthorized use of a P-Card\(^1\)—whether by the cardholder, other internal employees and/or outside parties, resulting in one or more acquisitions whereby the end-user organization does not benefit. This includes crimes such as a cardholder’s use of the card for personal gain, use of stolen cards, account numbers and counterfeit cards. Merchant fraud is another example, involving charges to the organization for goods or services not provided by the merchant.

- Misuse involves unauthorized activity by the employee to whom the card is issued. For example, misuse could include poor asset management resulting from buying a larger quantity than necessary, purchasing materials or goods of a higher quality than the organization would deem appropriate or buying from unauthorized suppliers. In these examples, the end-user organization receives some kind of benefit (e.g., it receives the purchased goods), but the employee has misused the card by not being compliant with internal policies.

---

\(^1\) Use of the word “card” within this report refers to either a physical card or a card account number (no actual plastic).
Liability often differs for fraud and misuse; for example, misuse is the responsibility of the employer. Fraud perpetrated on a Commercial Card is not covered under consumer protection legislation. However, card networks and/or issuers may provide some form of liability protection. An organization should review its P-Card contract to become familiar with the terms and conditions concerning fraud, such as liability waiver protection and chargeback rights.

**Integrating Deterrents in Program Design**

Appropriate controls should be integrated into a P-Card program from the beginning, during the design phase. Controls can also be strengthened or added to an existing program at any time, which is often necessary as a program grows or changes.

During the program design and program management phases, organizations can use a team drawn from multiple business functions to help secure consensus and support for the controls that the organization will integrate into the program. Functional representation may consist of procurement, accounts payable, finance/treasury, internal audit, information technology, as well as other areas. Examples of items this team should address include:

- a potential unique card design (if available) whereby the appearance of the plastic card readily distinguishes it from a consumer card to reduce confusion
- intended card distribution, including the appropriate approvals and training required prior to card issuance
- controls that are needed to regulate and monitor purchases
- transaction documentation requirements
- program reporting needs
- controls related to the accessibility of information and card data
- the strategy for testing the controls to ensure effectiveness

A cross-functional team approach will also facilitate a unified strategy relating to the types of purchases that are within the scope of the program, what constitutes misuse of the card and repercussions for policy violations.

**Prevention**

End-user organizations should use a variety of approaches to help prevent fraud and misuse, including:

- establishing roles and responsibilities
- ensuring separation of duties
- implementing appropriate policies
- documenting clear procedures
- utilizing systemic controls
Establishing Roles and Responsibilities

The roles and responsibilities for each individual involved in the P-Card program should be clearly defined to minimize gaps in accountability.

Program Management Team

The program management team (e.g., program manager and/or administrator) plays a key role and acts as the organization’s liaison to the card issuer. Responsibilities associated with the control environment include managing card issuance, maintaining related card controls, canceling cards, suspending accounts and program reporting.

Cardholders

As a key control for protecting the organization from outside fraud, cardholders should be required to complete appropriate training on policies and procedures prior to card issuance. Their responsibilities include maintaining the security of their P-Cards, using the card only for authorized purposes and reviewing their transactions according to the guidelines established for the program. Errors, discrepancies and potential fraud should be promptly identified and disputed. Cardholders must also ensure appropriate supporting documentation for transactions, including original receipts and any required approvals.

Approvers

Approvers (typically a cardholder’s supervisor or manager) are responsible for oversight. They monitor cardholders’ compliance with organizational policy and procedures. Like cardholders, approvers should be required to complete P-Card training. While each organization may define the approver role differently, specific responsibilities may include:

- ensuring cardholders have completed training on the proper use of the card
- reviewing cardholder transactions and supporting documentation on at least a monthly basis
- monitoring spending patterns and suppliers used, as a sudden unexplained increase in purchases or questionable suppliers may indicate a problem
- reporting instances of probable fraud or misuse to the appropriate party (e.g., program management team)

Card Issuer

As a partner to the end-user organization, the card issuer has fraud detection systems that are instrumental in identifying out-of-pattern purchases. Subsequently, its role includes alerting the end-user of any potential fraudulent activity and recommending appropriate actions.

Suppliers

Last, but not least, an organization’s suppliers have a role in fraud prevention and detection by keeping card data secure, in accordance with the Payment Card Industry Data Security Standard (PCI DSS). In addition, suppliers may be familiar with how and what an organization purchases, thereby able to recognize potential fraudulent purchases and notify the organization accordingly.
Ensuring Separation of Duties

Appropriate separation of duties related to program management tasks is a key factor in an effective control environment, one that is often a focus during program audits. In general, separation of duties provides a system of checks and balances, supporting policy compliance. For example, to prevent unauthorized account set-up, the person who handles an application for a new card (e.g., the program administrator) should not be the person who also receives the physical card from the issuer—unless additional controls and oversight for this process are established. Broadly speaking, risk to the organization increases when a particular employee:

- performs all steps of a critical process without appropriate oversight and/or
- has extensive access to more than one system (e.g., the card technology and financial systems) with the ability, for example, to download transactions from the P-Card system, import transaction data into the general ledger and, at any point, edit the transaction data

To ensure appropriate separation of duties, multiple employees generally need to be involved with key processes—each handling a specific portion—with system access for each employee limited to their respective duties.

Implementing Appropriate Policies

A P-Card policy provides the foundation for the control environment, establishing expectations for program participants and the program management team. End-user organizations must create card policies that align with program goals and objectives. Therefore, policies vary greatly by organization and can range from very general guidelines for card use to very specific attempts to address all foreseeable situations. Generally, policies prohibit activities such as personal use, cash access, transaction splitting and card sharing.

- Personal use is not permitted by most organizations due to corporate (i.e., organization) liability for charges placed on the card.
- Cash access, whether through an automated teller machine (ATM), convenience checks or a bank teller, is prohibited in most programs. Some organizations, however, do utilize this feature under some circumstances, such as within a One Card program for cardholders on business travel.
- Transaction splitting involves a merchant splitting a purchase that exceeds the cardholder’s single transaction limit into two or more smaller transactions to facilitate transaction authorization. Transaction splitting, whether requested by the cardholder or initiated by the merchant (and unbeknownst to the cardholder), circumvents an important systemic control.
- Card sharing by employees dilutes the organization’s ability to hold the employee accountable for card activity. Traditional P-Cards are issued in the name of an employee and that employee is responsible for the security of the card, as well as the transaction activity that occurs on it. In addition, merchants who diligently attempt to reduce card fraud by verifying the identity of the cardholder should decline the card if presented by someone other than the cardholder.

Policies also typically describe the job role or position that should be issued a P-Card, the targeted purchases and where P-Cards fit into the organization’s payments strategy.
It is likely that an organization’s P-Card policies will change over time as the program changes, matures and/or expands. As such, the organization should determine the department or business unit responsible for managing the policy. Thought should also be given to the process for communicating policy changes to the organization at large and, especially, card program participants. Communication methods may involve broadcast voicemail messages, e-mails or resources and messages posted to the company’s Intranet.

**Documenting Clear Procedures**

Procedures support the policies and should be reviewed and revised as policies change. Procedures intended for cardholders and their managers should be easily accessible—located, for example, on the organization’s Intranet. Conversely, procedures governing the activities of the program management team can be stored within the department assigned this responsibility, limited to designated staff. Electronic procedures are easier to update and maintain than paper-based manuals, reducing the risk of employees using outdated materials.

**Procedures for Program Participants**

Procedures and other program information typically address the following core topics:

- **General information about the program**
  - Background
  - Statement of purpose, benefits to the organization
  - Contacts
- **Roles and responsibilities**
  - Cardholders
  - Approvers
  - Program management team
  - Issuer
- **Obtaining a card**
  - Process, requirements and authorization
  - Training
  - Card activation
- **Account/card security**
  - Retention and storage
  - Avoiding scams (e.g., phishing)
- **Card usage**
  - Targeted transactions
  - Prohibited transactions
  - Purchasing procedures and related policies
  - Documentation requirements
  - Procedures for declined transactions
  - Requesting temporary or permanent changes to card controls (e.g., limits)
• Transaction review and reconciliation
  – How to use the P-Card technology
  – Accounting distribution process
  – Disputes and potential fraud
  – Oversight and approval
  – Records retention

• Cancelling a card (e.g., account closure)
  – Lost or stolen cards
  – Exit procedures, including card retrieval

As indicated above, procedures should define the authorization required for card issuance. The authorizing individual should be in an appropriate position of responsibility within the organization. Some organizations require the authorizing manager to have budgetary responsibility. As a best practice, organizations should require employees (cardholders and approvers) to sign an internal agreement form (aka Cardholder Agreement) prior to card issuance that specifies their card-related responsibilities and the possible consequences for non-compliance.  

A typical agreement serves to confirm and document that an employee:

• has been informed of the policies and procedures governing the card program
• understands that violations of the policy may result in disciplinary action, including possible employment termination
• agrees to make restitution to the organization for personal use
• will surrender the card on demand

Any such agreement should first be reviewed by the organization’s human resources and/or legal department to ensure adherence with employment laws and internal policies.

It is also a best practice to mandate training on organization card policies and procedures prior to card issuance—for both card applicants and the designated approvers. An effective training program should not be overlooked as an important tactic to prevent fraud and misuse. An organization may also want to include a testing component within its training program to determine an employee’s comprehension of policies and procedures.

An organization’s documentation requirements to support card transactions may differ by purchase type, but they must satisfy the requirements of applicable taxing authorities.

**Procedures for the Program Management Team**

Procedures followed by the program management team should be documented as well, aligning with and complementing the procedures set forth for program participants. Topics generally include the following, reflecting the perspective and duties of the program management team:

• Program goals and metrics
• Card/account requests, set-up and issuance

---

2 A sample agreement is available to NAPCP members in the online Resource Center at www.napcp.org/resourcecenter.
• Training (for program participants)
• Account maintenance (temporary and permanent changes to card limits/restrictions)
• Monitoring activities
• Interfacing P-Card data with other systems, such as the finance system
• Payments to card issuer
• Program reporting and analysis
• Cancelling cards (e.g., account closures) and card collection/destruction
• Using the administrative tools within the P-Card technology
• Program risk analysis
• Contract with card issuer

If there is not an automatic interface between the P-Card system and human resources’ data to ensure only active employees have cards, a scheduled review should be performed to identify terminated employees and those on leaves of absence. Even if an organization has a well-defined exit process that includes a step for card retrieval, some employees leave their jobs unexpectedly. The program management team must be kept informed on employee status changes, so that cards can be suspended or cancelled accordingly.

In addition to monitoring employee status, some basic steps are needed to prevent cards from falling into the wrong hands prior to distribution to the employee. There is a risk of cards being pilfered in transit between the issuer and the recipient. Fortunately, it is generally difficult to activate a card without the secure information required by the issuer. Nevertheless, the employee who receives a card should be expecting and watching for new cards, becoming suspicious if the cards are not delivered in a timely fashion or appear to have been tampered with during transit. When using internal distribution channels to deliver a card to an employee, pilferage can be reduced by packaging the card to appear as normal internal correspondence.

**Utilizing Systemic Controls**

Appropriate systemic card controls should be implemented for each P-Card account based on the cardholder’s business needs while aligning with program goals and policies. Systemic card controls provide an automated approach to controlling purchases, helping to prevent fraud and misuse, and supporting card use for targeted transactions. End-user organizations typically employ several of the following systemic controls:
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single transaction (single purchase) limit</td>
<td>Maximum dollar amount allowed for a single transaction</td>
</tr>
<tr>
<td>Monthly (cycle) and/or daily spend limit</td>
<td>Maximum dollar total allowed per designated timeframe</td>
</tr>
<tr>
<td>Velocity controls (e.g., daily transaction limit)</td>
<td>Limits the number of times a card can be used within a specified period of time</td>
</tr>
<tr>
<td>Merchant category code (MCC) blocks</td>
<td>Prevents card usage with suppliers in prohibited industries (e.g., casinos, jewelry stores, etc.)</td>
</tr>
<tr>
<td>Storefront merchant blocking</td>
<td>Prevents card usage with a particular merchant and/or merchant site</td>
</tr>
<tr>
<td>ATM blocking</td>
<td>Prevents ATM access for cash advances</td>
</tr>
</tbody>
</table>

Systemic controls may differ slightly by card issuer; some may not be available from some issuers.

While use of systemic controls is a best practice, excessive restrictions may reduce the benefits of P-Cards; for example, excessive MCC blocks may result in legitimate transactions being declined. Experiencing and resolving declined transactions for legitimate business purchases are time-consuming for cardholders and the program management team alike, impacting the acquisition process cost.

**Detection**

Complementing preventative measures are detective techniques, which are equally important. They include auditing, transaction reconciliation and program reporting.

**Auditing**

Above all, audits should be meaningful, tailored to the organization’s unique program. There are two primary types of audits: process audits and transaction audits.

Process audits are usually conducted by auditors to test the effectiveness of program controls. One purpose is to discern whether program participants and the program management team understand and follow documented procedures; for example, an auditor may interview cardholders. Attribute testing may also be used to assess the internal controls; for example, a personal purchase on the card is traced through the process to see how various controls operate to detect the activity. If the controls are found to be ineffective, modifications or supplemental controls may be necessary. Process audits generally occur annually, but may vary depending on the stage of a program, previous audit results or other factors.

Transaction audits, on the other hand, tend to be conducted by a variety of employees on a regular basis. They focus on card activity (transactions and supporting documentation) to identify potential fraud and misuse, and determine compliance with policies. The sample selection methodology should be consistent with the organization’s internal audit procedures. However, cluster sampling, in which every nth cardholder is audited rather than every nth transaction, may allow inappropriate activity to go undetected.
Transaction audits should be strategic, focusing, for example, on:

- high-dollar purchases
- new cardholders’ purchases (to assess compliance with policies and procedures and to determine if re-training might be in order)
- transactions with prohibited suppliers and/or MCCs
- purchases occurring during non-business hours (e.g., weekends)
- cardholders with high transaction volume and/or spend
- purchases that are billed to clients
- cardholders with recurring disputes

All cardholders should be audited at a minimum of once a year; however, many organizations prefer a greater frequency. Manually auditing every transaction for every cardholder every period reduces the process savings inherent to P-Cards. While this may be a common approach during a program’s implementation stage, a better long-term approach is for an organization to review the cost-versus-benefit of various approaches and consider its level of risk tolerance. Does the organization want to spend, for example, $200 to find a $20 issue? If an organization with a manual, 100-percent-audit process finds few—or even no—serious infractions, it may want to consider something other than a “100% approach.” It should adjust its process to suit its appetite for risk. In addition, an organization should explore automated tools to aid the audit process, ranging from common computer programs (e.g., Microsoft Excel) to robust auditing technology solutions.

Areas that might be included for review in an auditing process are:

**Approvals**
Were the proper approvals obtained for:
- card issuance?
- account maintenance?

**Documentation**
Are receipts (or other supporting documentation):
- compliant with organization policy?
- detailed enough to identify what was purchased?
- altered or fabricated in any way?
- missing?

**Expense Control**
Did the purchaser:
- obtain favorable (or contract) pricing from the supplier?
- use preferred suppliers?
- buy an appropriate quantity?
Reviewing, Reconciling and Approving
As noted previously, one of the first lines of defense against fraud is the cardholder. Through a timely review of the card activity and a reconciliation of the transactions (matched back to documentation, receipts, purchasing records, etc.), unauthorized charges can be identified and disputed or the card reported stolen or compromised. This process is also effective in identifying merchant fraud.

Subsequent transaction review by the designated approver serves as another detective layer (and a first line of defense against cardholder fraud).

Organizations typically require cardholders to complete the review and reconciliation process, followed by management approval, on at least a monthly basis. P-Card technology systems today allow participants to review posted transactions daily, if desired.

Creating and Analyzing Reports
Development of a standard reporting suite can keep management aware of card usage and compliance with policies and procedures. Reports, in conjunction with the ability to query transaction data and produce ad hoc reports, can assist in the early detection of inappropriate or fraudulent card activity, supporting the audit process. Some of the reports useful for this purpose, especially when analyzed regularly (e.g., at least monthly), are described below.

Declined Transactions
A review of declined transactions may reveal recent fraudulent attempts. For example, if someone has the card number, but does not have the card verification code or expiration date, multiple declines for these reasons may indicate that someone is using a trial-and-error approach. Declined transactions for blocked MCCs may also mean fraud or attempted misuse by the cardholder. Particular attention should be paid to those MCCs that involve cash access.

A declined transactions report is useful for multiple reasons. While declined transactions certainly may indicate potential fraud or misuse, repeated declines could indicate issues with the card program that may be solved through additional cardholder and/or merchant training.

Activity Analysis
A review of card transactions to identify unusual activity may be an early indicator of misuse or fraud. The program management team and/or auditors should review transaction detail for a high volume of charges, particularly those of a retail nature, which may indicate a stolen or counterfeit card.

Multiple transactions by the same cardholder with the same supplier, especially on the same day, should be evaluated to determine if the cardholder is attempting to circumvent the spending controls placed on the card.

Another type of analysis might focus on cash-convertible activity, such as gift cards or certificates, which are typically purchased in even-dollar increments ($20.00, $50.00, etc.).

As with transaction declines, an organization should use an activity analysis as a starting point for investigative purposes rather than jumping to conclusions without additional facts.

Disputed Charges
A history of disputed charges may support the need for additional cardholder training on proper purchasing procedures, but it may also mean improper purchasing behavior.
A high frequency of disputes involving a single merchant may also indicate merchant fraud. This pattern might not be visible without analyzing dispute patterns for the entire organization.

**Account Listing**
The roster of employees issued cards should be reviewed to determine current need based on each employee’s job responsibility. This report can be made more useful by indicating cards that have not been used within a specified timeframe, such as six months. Periodic review by management will create an awareness of employees with active (and inactive) P-Cards, helping to identify cards that may no longer be needed.

Related to an account listing are reports of new P-Cards and cancelled cards (e.g., accounts opened or closed during previous month) to ensure that cards were:

- opened or closed appropriately (e.g., an intended cancellation did, indeed, occur) and
- not obtained or closed outside of the established processes, without the knowledge of the program management team

**New Account Activity**
To ensure cards have not been issued fraudulently, a monthly report of new account activity should be reviewed by management. This report provides the assurance that those who fulfill a P-Card Administrator role have not ordered cards for the purpose of fraudulent activity (e.g., bogus employee names, their own names, etc.)

**Conducting a Risk Analysis**
On a regular basis, such as annually, an organization should evaluate the potential risks within its program, as this supports the audit process. Some organizations, especially those in the public sector, may determine that additional controls, which often result in a higher process cost, are acceptable in an effort to prevent negative media exposure. Other organizations may be more risk tolerant. In either case, as part of a regular review, an organization should:

- evaluate all P-Card processes, including tasks performed by the program management team
- determine who performs each step and the possible risks of each process
- document the existing mitigating controls
- identify the tasks that need separation of duties and/or oversight
- take the necessary actions to close any gaps in the controls, implementing or revising procedures accordingly

With the implementation of new controls or control revisions, an organization should recognize that staff may need additional training to handle any new duties.

**Conclusion**
All payment methods present certain risks to an organization. Establishing and maintaining an effective control environment for every payment method, including P-Card, is a must. Many different controls, as described within this report, are available to end-user
organizations to help minimize card fraud and misuse and protect the organization from loss. However, it is possible to both under- and over-control a P-Card program.

While an organization may be tempted to try to lock-down every conceivable element of risk, there is also a corresponding tradeoff in doing so. Ultimately, an organization needs to weigh the costs and benefits of its program controls, striving for an appropriate balance to fit its needs. Those unable to find this balance risk failure to achieve the maximum benefit from their card programs.

As indicated in the report overview, a P-Card program tends to trade up-front approval for improved back-end accountability. Nevertheless, P-Cards can be just as “safe” as other payment methods, offering certain protections (e.g., liability waiver insurance, chargeback rights, dispute process, etc.) that other payment methods do not.

**Additional NAPCP Resources**

Additional resources related specifically to controls are available from the Resource Center at [www.napcp.org/ResourceCenter](http://www.napcp.org/ResourceCenter) (section on Controls, Audits, Compliance and Fraud). Most items are exclusively available to members. To become a member, visit [www.napcp.org/JoinNow](http://www.napcp.org/JoinNow).

Fraud prevention, controls utilized by end-user organizations, as well as financial loss due to P-Card fraud, are routinely a topic of NAPCP polls. Poll results, many of which include educational tips, are accessible to NAPCP members and complimentary subscribers and can be found at [www.napcp.org/Polls](http://www.napcp.org/Polls).

The NAPCP also offers a guide for purchase, *Purchasing Card Essentials: The NAPCP's Guide to Establishing and Managing a Program*, with more than 125 pages of content, including graphs, instructions and examples. For details, visit [www.napcp.org/P-CardEssentials](http://www.napcp.org/P-CardEssentials).

**About the NAPCP: Advancing Commercial Card and Payment Practices Worldwide**

The NAPCP ([www.napcp.org](http://www.napcp.org)) is a membership-based professional association committed to advancing Commercial Card and Payment professionals and industry practices worldwide. Serving a community of more than 19,000, the NAPCP is a respected voice in the industry and an impartial resource for professionals at all experience levels in the public and private sectors. The NAPCP provides unmatched opportunities for continuing education and peer networking through its conferences, Regional Forums, webinars, website, virtual demonstrations, newsletters and regular communication. The association sponsors research and publishes timely and relevant white papers, survey results and articles. The NAPCP offers a Certified Purchasing Card Professional (CPCP) credential. Visit [www.napcp.org](http://www.napcp.org) to learn more about Commercial Card and Payment programs in general, the value of membership, current member demographics, upcoming events and benefits of becoming a year-round partner sponsor. In addition to membership, the NAPCP offers complimentary subscriptions to its website, with partial access to industry news, research results, polls and other resources. To become a member, visit [www.napcp.org/whyjoin](http://www.napcp.org/whyjoin).