P-Card Newsletter

Volume 3, issue 2 **July 2012**

In FY12, P-cards yielded over 80,000 transactions equaling over 26 million dollars. Fifty-one BC P-cards were compromised but not one physical card was lost or stolen. This compromised figure has more than doubled from FY11. Over eight million Americans had their credit cards or ATM cards compromised in 2011 in the same way. This Newsletter is dedicated to help our cardholders and administrators prevent this from happening.

Deactivating P-cards of Former Employees: One of the Most Important Things You Need to do for Your Department.

With recent changes in staff and new positions created, please make sure that all p-cards of former employees, as well as closed grants, programs or old dept p-cards are deactivated on PeopleSoft. This will prevent unauthorized purchases. Unauthorized purchases can be made on any open p-card and will only be noticed after the information is fed into PeopleSoft a few days later. In FY12, two p-cards from former employees were compromised and noticed months later. Don't let this happen to your department.

For detailed instructions on how to see all active p-cards and how to deactivate them in PeopleSoft, go to www.bc.edu/procurement >Purchasing Card Program> P-card lab for PeopleSoft financials.


How Did They Get My P-card Number? My P-card Never Left My Pocket!

People rarely carry cash so street robbing is no longer lucrative. Every year criminals think of more inventive ways to get your number while VISA, MasterCard and AMEX become more diligent about keeping it secure. You may wonder, how can a criminal guess a 16 digit number? They are not just guessing but work in an organized, criminal ring dedicated to capture, sell and use your credit card. Previously, criminals would just go through your trash, looking for credit card receipts but with the elimination of full credit card numbers on those receipts, they have become more creative.

Here's how they do it:

1. **Phishing**: An attempt to acquire information such as usernames, passwords, banking and credit card numbers usually by e-mail or instant messaging. The message asks you to click on to a site which is almost identical to your bank's to verify information.
   Here's what you can do: Don't clink on to anything that tells you to "verify your information here". Look at the link carefully, it will have added words, (dot com may appear twice): i.e.: www.bankofamerica.com.verifing.com.
   When in doubt, call your bank directly.

2. **Vishing**: Like Phishing except the criminal will call you directly on your phone, pretending to be from your bank or credit card issuer.
   Here's what you can do: Your bank or credit card issuer will NEVER call you asking for personal information. Never trust *anyone* who calls you and asks for your social security #, bank account # or credit card information.

3. **Spyware**: Computer software inadvertently installed on your computer when visiting or accidently visiting certain websites. Once installed, your every move can be tracked, including signing on to your bank website and entering your secret passwords as well taking stored information from the desktop and access to your email.
   Here's what you can do: Install anti-spyware on your home computer. BC already has this tool installed in work computers. However, there was an incident where an entire department's p-card numbers were stored and stolen off the desktop from Internet criminals. Run your "Identify Finder" program everyday to ensure sensitive information is not stored anywhere vulnerable. Store information in a secured server behind a firewall. Do not put credit card #'s in e-mail!

4. **Skimming:** Typically an "inside job" from a dishonest employee by a legitimate merchant who steals your credit card number directly from you. This usually happens in bars or restaurants where you are not in view of the transaction.
   Here's what you can do: Avoid outside shopping with your p-card. In general, you are more protected using a p-card on the internet. Please make sure the website you are using is a secure one. In the address bar, the website should begin with "https". The "s" at the end means it's a secure, encrypted site.

5. **Data Breach:** Trusted businesses that have your personal information stored may fall victim to being hacked. A data breach also takes place when a computer, media storage device or box of files is lost, stolen or misplaced.
   Here's what you can do: When a company is breached, the cardholders are usually notified or it is publically announced on the News. Please do not ignore that notification. If your p-card is involved in a breach, please contact pcard@bc.edu. Five P-cards in FY12 were compromised when a company called "Global Payments" was breached.

6. **Social Networking:** Thieves can now get personal information about you directly from your Facebook page. (Date of birth, maiden name, city, zip code, etc.) They can use that information and pretend to be someone else to get more information from you or your network of friends. In addition, they can now answer any secret questions under a "forgot pass-word" field.
   Here's what you can do: Please keep your Facebook, Linked-In, Twitter, My-Space, etc settings private. Don't answer personal questions from someone you do not know (or *think* your know)

   The most proactive thing you can do: **CHECK YOUR STATEMENT every month. If possible, check your p-card purchases on a weekly basis on US Banks' *Access-on-line* even if you have no p-card activity.**

In-Store Shopping VS On-Line Ordering

It's a beautiful day. Your department needs some things so the administrator decides to run to Staples. Last fiscal year, 242 Boston College personnel ran to Staples in Newton, Waltham, Cambridge, Watertown, Needham and other stores around the area. Each person spent on their department p-card an average of $142.00, totaling $34,320.00. Occasionally, there may be a need for University personnel to pick up goods rather than wait for them to be delivered but these occasions should only be the exception to the rule. In order to promote operational efficiency, please consider the following:

1. **Order from WB Mason** and other contracted vendors directly from the Procurement website to ensure the deepest contract discounts as well as the full range of product available.
2. **Save on pricey gas and valuable time**. A five minute trip to the Chestnut Hill Mall can turn into a fifteen minute excursion in traffic and parking. Time is also taken to walk and browse adding to the cost of the transaction.
3. **Organizing your receipts**: You won't have to worry about misplacing receipts when it's time to reconcile your p-card when ordering online from contracted vendors. Receipts are not required for purchases less than $999.00 from WB Mason and other contracted level 3 vendors but outside vendors require receipts, regardless of the price, for Audit.
4. **Taxes paid** for purchases at Staples for FY12 totaled $728.00. Orders placed with WB Mason will never include taxes since the University is exempt from all sales tax.

Unnecessary Taxes: Another reason why contracted vendors should be used. Total University sales tax paid to outside, non-contracted vendors equaled almost $26,000 for FY12. This is an unnecessary and avoidable loss of University funds. Whenever possible please use our contracted vendors.