Greetings from the staff of Treasury Operations

We would like to extend warm holiday wishes to all the departments that work with Treasury Operations. We have appreciated the hard work you have put into managing your cash, checks, and credit card processing. 2008 has been a crazy year and a busy year for Treasury Operations as well as for our nations economy. We have worked on keeping credit card holder data secure, streamlining your deposit processes with remote capture, and protecting the university from one of the worst financial meltdowns this country has witnessed.

Now we look forward to a new year that still may be busy and will require all of us to work together in making Indiana University a secure and efficient environment to transact business.

So, during this time of holiday cheer we hope you re-energize yourselves through rest and relaxation.

Happy Holidays from all of us at Treasury Operations!

Dennis Reedy, Cheryl Shifflett, Ruth Harpool, Diane Thrasher, David Newsom, Kim Stuart, Josh Welsh

---

PCI DSS Self Assessment Questionnaire

By now all of our merchants should have completed the Trustwave Trustkeeper Payment Card Industry Data Security Standards Self Assessment Questionnaire. We want to thank all of you for completing it. We want to also remind you that PCI DSS compliance is a 24/7 365 day issue and although you have completed the questionnaire there is still work ahead of you in keeping cardholder data secure. Those of you that have terminals make sure you read our section on terminal maintenance and those of you with specialty systems make sure you update your Self Assessment Questionnaire once you move over to the new network. We also want to make sure you all know that you will be required to complete the SAQ on an annual basis.

If you have any questions about the PCI DSS Self Assessment Questionnaire please contact Payment Card Services at pmntcards@indiana.edu or by phone at (812) 855-0586.
PCI DSS - Document Storage & Retention

Okay, so you know not to keep cardholder information when you don’t need too but, what about all the past paper documents that have cardholder information on them. What are you supposed to do with it? Here are some steps that you should immediately take to secure the data contained on those documents:

♦ Documents must be destroyed after two years. The only acceptable method of destruction is by cross cut shredding the documents. Any documents waiting to be shredded must be enclosed in a locked bin. If you have contracted with a confidential destruction company it is your responsibility to obtain verification that items given to them to be destroyed have actually been destroyed in a secure manner and within the two year time frame.

♦ Documents in storage must have cardholder information (credit card #) redacted by blacking out all of the number except the last four digits. Those documents must be stored in a secure environment such as a locked office inside a locked desk drawer, cabinet, or vault. Any current documents must not contain full cardholder information. If the document has such information the portion of the document that contains the cardholder data must be redacted as mentioned above. Note: when redacting the cardholder credit card number it may still show through in which case the original must be Xeroxed, then destroy the original and keep the copy. Another method to redact credit card numbers is by punching holes through the numbers.

♦ If you have applications, enrollment forms, or any other document that collects customer and credit card information you may need to redesign the document so that the credit card information can be easily destroyed without having to discard other pertinent customer information you may need.

Remember it is your responsibility to protect cardholder data! By following the steps above you will be well on your way to being in compliance with the Payment Card Industry Data Security Standards (PCI DSS) as it pertains to storage and retention. Being in compliance is an on-going process which in the long run will protect you, your department, and Indiana University. If you have any questions or need further information please contact Payment Card Services at pmicards@indiana.edu.

Stop to see the forest this Holiday Season... their pine fragrance fills the holiday air... stop a little longer under the mistletoe... keep a smile on your face and enjoy friends and family... let the stars shine brightly on your festive occasions!
**Policy VI-450: Establishing and Generating Revenue Producing Activity**

Per Policy VI-450, “Any revenue producing activity (RPA) must be approved by the campus business officer. An RPA is established when revenue is generated for the sale of products and/or services provided by the university and or university employees...When planning or approving business activities, Deans, Department Heads, and other appropriate administrators should ensure that these activities are consistent with this policy. Departments that do not follow the guidelines set forth in this policy will at a minimum be held responsible for any fines or penalties externally imposed (an excerpt from policy I-450).”

Recently, Payment Card Services has been contacted by several departments that have events scheduled in which they want to accept credit cards, so we thought it appropriate to make everyone aware of the steps involved before you decide to make credit cards one of your payment options.

To establish a new Revenue Producing Activity (RPA) account the department must:

- Schedule a preliminary review meeting/discussion with the campus business officer before commencing with the following steps to establish an RPA account;
- Complete an RPA Questionnaire
- Create a business plan
- If a recharge center, prepare a schedule of rate calculations for the operation
- Submit the questionnaire, business plan, completed Conflict of Interest Disclosure Statement, if applicable, and any supporting paperwork to the campus business officer for approval.

When Treasury receives a routed questionnaire (RPAQ) from campus administration, we review the portion of the questionnaire regarding the departments intended revenue processes. Treasury may require the department to answer additional questions for clarification, so that we can get a good picture of what the departments revenue process should be. After our review of the information Treasury makes a recommendation of how the department should process the revenue and approval is contingent on the departments compliance to those recommendations. If our recommendation is to process revenue by credit cards the department must then contact Payment Card Services for implementation and setup at which time we will direct you on the process of accepting credit cards which can take up to two weeks from that point.

**Pin Debit Card Refunds-Fraud**

If your department processes debit cards by having the customer enter their PIN number into a PIN pad, you may no longer process PIN based Debit card refunds due to the high risk of fraud.

A common example of this fraud is a situation where a criminal or a merchant’s employee processes PIN Debit refunds via an unattended or unsecured credit card terminal, then goes to an ATM to withdraw the credited funds before any merchant detection or correction can occur. Many merchants and their banking partners have suffered significant losses due to this tactic. This is yet another reason why it is important to comply with PCI DSS as it pertains to securing equipment.

Our credit card processor Elavon has, as of September 8th, 2008 disabled the funding capability of our merchants to process PIN Debit refunds. The terminals will no longer allow the processing and will generate a system response message of SVC NOT ALLOWED on your terminal.

Wondering what to do when you need to give a refund to a customer who used their debit card?

You must now process the Debit card refund just like you would process a Credit Card refund. This is called a signature based debit transaction and the refund is not immediate therefore reducing the risk of fraud.

If you have any questions concerning this information please contact Payment Card Services and we would be happy to address them.
Credit Card Terminal Maintenance & Troubleshooting

Legend has it that around this time of year credit card terminals start acting like a little haywire. It never falls in the midst’s of the hustle and bustle of students leaving and employees eager for the holiday break the terminal does something it had never done throughout the year. So this is a reminder to not lose your composure as Payment Card Services is here to help. By contacting us you stay in PCI DSS compliance and we keep track of problems that may occur with our terminals. Here are some rules to follow when your terminal is not functioning properly:

◆ Read the terminal screen to see what the error message is saying. This helps us to figure out what is going wrong.
◆ Call Payment Cards first at 855-0586 to get help; if we are not available then call the helpdesk at 1-800-777-7240.
◆ Don’t try to be a handyman/woman; do not take the terminal apart or try to fix it yourself. All replacement terminals will cost you a fee of $89.

International Wires—Things to know about International Wire Transfers

International banking structures vary by country so the detail needed for every wire transfer request can vary by country and sometimes by bank. There is no such thing as a routing number in international banks so other methods of identifying banks are necessary. Here are the critical pieces of information that you should have before requesting an international wire transfer.

Remember: It is very important that descriptions be Accurate and as detailed as possible. Even an incorrect spelling can cause a wire to be returned, not applied to the correct account or in some cases not applied at all.

Name of Bank
Bank City
Bank Country
Bank SWIFT code (see below for definition)
IBAN (see below for definition) required for Euro payments within Europe
Bank Account Number
Name of Recipient
Recipient Address, City, Country
Currency Type
Amount

Definition of SWIFT: Society for Worldwide Interbank Financial Telecommunication. Every bank has a SWIFT code. A SWIFT code is required to send international payments.

Definition of IBAN: International Bank Account Number. The IBAN is a combination of a country code, a country number, a bank identification number (BIN), and customer account number.

If you have other questions please call Treasury at 812-855-9268.
Remote Capture Troubleshooting

We have some problems that have occurred in the recent past with departments using Fifth Third Direct Remote Capture Scanners that we wanted to bring to your attention. When scanning checks, the process should be very smooth from start to finish, if it is not, PLEASE let us know! Some of the problems we have encountered recently include:

<table>
<thead>
<tr>
<th>PROBLEM</th>
<th>SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long delay between checks being</td>
<td>Changed USB jack</td>
</tr>
<tr>
<td>Having to hand key majority of</td>
<td>Clean scanner</td>
</tr>
<tr>
<td>Scanner jamming</td>
<td>Clean scanner/ if no success, call</td>
</tr>
<tr>
<td>Check numbers not scanning</td>
<td>Clean scanner</td>
</tr>
<tr>
<td>Required to change password</td>
<td>Call the help desk 800-589-5355</td>
</tr>
<tr>
<td>No spray line on back of check</td>
<td>Sent new ink cartridge</td>
</tr>
</tbody>
</table>

We also have “human” errors that sometimes occur, the ones we see most include:

<table>
<thead>
<tr>
<th>ERROR</th>
<th>SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forgetting to transmit scanned checks</td>
<td>Remember to hit the transmit button on the bottoms of the last page</td>
</tr>
<tr>
<td>Shared passwords</td>
<td>NEVER share your password!!! NEVER!</td>
</tr>
<tr>
<td>Scanned check twice</td>
<td>Make sure to read the pop-ups that appear NEVER accept a duplicate</td>
</tr>
<tr>
<td>No endorsement on checks</td>
<td>Always remember to endorse the checks prior to scanning</td>
</tr>
<tr>
<td>Timing of FIS document</td>
<td>Do your FIS doc AFTER you scan, on the same day you scan</td>
</tr>
</tbody>
</table>

If your scanning isn’t running as smoothly as you think it should, or if you have general questions, please call us! We are here to help!
Diane Thrasher 812-855-8587  dthrash@indiana.edu
David Newsom 812-855-9457    wnewsom@indiana.edu

Can you Guess Who We Are in Treasury Operations?

Throughout the newsletter are ornaments with Treasury Operations Staff pictures on them. Can you guess who we are and what we do? Each ornament has a number by the picture. The first email we get with the correct answers will win a Treasure from Treasury Operations. Only one entry per person. In order to win the Treasure your answers must only be sent to the following email: treasury@indiana.edu
This is your chance to see if you know us. After the winning email is received Treasury Operations will send out the correct answers so that everyone can get to know our staff. Good luck!
Remote Capture

Remote capture is a system which will enable departments to immediately deposit checks your department receives, on-site by scanning the checks through a check scanning device, your department will then transmit the deposit directly to the bank. This helps secure and protect checks, and also allows the funds to be deposited into an IU bank account immediately. Once deposited, the check images as well as other reports will be available for your needs for a limited time. Here is what some of our current users have to say about Remote Capture:

- Easy, Easy, Easy! I love it! It’s so simple to use and so fast!
- Remote capture is great! Not only is it faster and more efficient, it also solves a number of security issues. How did we live without it?
- I was apprehensive about starting the remote capture. Another thing to learn! But having used it for several months, I really like it.
- I love the remote capture, it is so easy (and fun) to use. I have not had any problems thus far. I love not having to do the accountable mail pick up request, and the fact that we can easily see our deposits and transactions is great.

Contact Diane Thrasher at dthwash@indiana.edu to find out more.

Revenue Processing Training

As stated in the Revenue Processing Policy VI-120, the Office of the Treasurer will hold periodic training sessions for all employees involved in revenue processing. These training sessions will alternate across campuses. A one time face to face attendance at a training session is mandatory for anyone processing revenue. If no training session is scheduled, prior to the inception of revenue processing, you must take the online tutorial. We are making every attempt to schedule the training sessions so that they can accommodate as many of your employees as possible without disrupting your daily business activities. All sessions will last two and a half hours.

More training dates coming soon!

If you have any questions concerning the Revenue Processing Training please contact Diane Thrasher. You can reach her at dtrash@indiana.edu or 812-856-8587.

Treasury Information Highway

◆ CHARGEBACK UPDATE: MasterCard is adjusting timeliness requirements for electronically authorized transactions. Transactions settled after 7 days from authorization are subject to potential chargeback’s if the cardholder account is not in good standing. This change does not have any impact on interchange qualifications.

◆ Found a lost or stolen credit card lately? Wondering what to do with it? First, be a good citizen and if you know the customer call them to let them know you found their card. Second, if you don’t know who the card belongs to then turn it over to campus police. Doing this gets the card out of your possession and the police may be able to find the owner if they reported their card lost or stolen.

◆ Treasury issued Endorsement Stamp: Treasury is in the process of issuing new endorsement stamps to certain locations. If you currently send your deposits though the Bloomington Bursar, please make sure the endorsement stamp you are using has a large 2010 on it. The old stamps that need replaced will have a 010. Please provide: Main contact name & phone number, e-mail, department name, and campus address.

To: Treasury@indiana.edu
Subject line: Endorsement Stamp (your department)
What’s In Treasury—Services We Can Offer

Treasury Operations is always available to provide training sessions as well as information on various topics and services we can offer. Whether you are new to IU, new to the position, or would just like to understand our services better, Treasury Operations can help. You can arrange training through Diane Thrasher at dthrash@indiana.edu, and she will set up a time for Treasury to meet with you and/or your staff. Some of the topics covered in each area’s training are:

**Payment Card Services**
- Electronic Commerce
- Fraud/Chargeback’s
- Electronic Business
- IU Pay
- PCI DSS

**Banking Services**
- Banking Operations
- ACH & Wire Transfers
- Fraud Prevention & Detection
- Lockbox
- Remote Capture
- Cash Handling

**Important Phone Numbers**
- IU Money Movement/Banking Services: 812-855-9268 moneymov@indiana.edu
- IU Payment Card Services: 812-855-0586 pmtrcards@indiana.edu
- 24 hr. Terminal Help Desk (Credit Cards): 1-800-777-7240
- Voice Authorizations (Visa & MC): 1-866-401-4852
- Voice Authorizations (Discover): 1-800-347-1111
- Voice Authorizations (Amex): 1-800-528-2121
- NOVA Customer Service (Tara Dyer): 1-800-725-1245 ext. 8091

**Let Us Know**

We want and need your feedback in order to make this a more useful publication. Please submit any ideas or issues you would like to see addressed in this publication to the Office of the Treasurer, Treasury Operations at dthrash@indiana.edu. Use the subject Newsletter Feedback.

If you would like to be added to or deleted from the newsletter distribution list, please let us know. You should email your name, title, department, campus address, phone, fax and email address to dthrash@indiana.edu.