Payment Card Digest
Payment Card News for University Employees

Understanding Your Statement
What do those numbers mean on your monthly merchant statement?

For Payment Card Account Managers, or their Accounting Staff, downloading your monthly statement from the Wells Fargo Merchant Services ClientLine website and checking it for accuracy is an important duty. This statement provides a record of submitted transactions, adjustments, and chargebacks. Your monthly merchant statement is also a great reconciliation tool between what Wells Fargo Merchant Services is reporting and what EFS is showing. But what do all the figures on your statement mean, and how should you reconcile? Taking a look at the summary cover page of the statement is a good first step.

See Sample Statement »

Service Provider Responsibilities

In our world of business models and applications that support (and even encourage) third-party payment card service providers, it is important to remember the following points:

1. Not all service providers recognize their active role as a payment card service provider, and this lack of awareness could potentially put the University at risk.
2. Utilizing third party service providers does not absolve you of all your payment card compliance responsibilities.

Merchants must ensure that third party service providers are compliant with the Payment Card Industry Data Security Standards (PCI DSS). Compliant service providers have undergone an audit and have been found to be in conformity with the PCI DSS. Compliance with PCI DSS helps to prevent credit card fraud through increased controls around data and its exposure to compromise. So before you sign on with a payment card service provider, contact Accounts Receivable Services (ARS) at pmtcard@umn.edu for assistance with this process.

See Additional Information on Service Providers »
The Payment Card Inventory List

It is important to maintain an up-to-date Cardholder Data Environment (CDE) and keep track of all of the various components that make up your environment. Keeping a proper payment card inventory list can seem like more trouble than its worth—but this document is an essential part of any merchant account’s compliance, and is required by the Payment Card Industry Data Security Standard (PCI DSS) under Requirement 2.4.

The PCI DSS requires areas that process payment cards to “Maintain an inventory of system components that are in scope for PCI DSS.” This inventory list should include a listing of components/devices, descriptions of the location of each item and its function, as well as serial numbers or unique identifiers. It is also a requirement that this list be reviewed on an annual basis and updated as needed.

Keep in mind that the requirement to maintain an inventory list will be very difficult to maintain until you fully practice PCI DSS Requirement 1.1.3 which requires you to maintain an updated cardholder data flow chart to showcase all the controls that are in the CDE and classify what is in-scope and out of scope for your CDE.

See Inventory List Templates »

If you suspect loss or theft of any material or records that contain cardholder data, contact the University Information Security (UIS) Incident Response Team immediately at (612) 301-4357 or abuse@umn.edu.

This email was sent to all Payment Card Managers and IT Professionals on behalf of Accounts Receivable Services, a unit within the Controller’s Office of the University of Minnesota. Please read the University of Minnesota’s mass email privacy statement.

©2015 Regents of the University of Minnesota. All rights reserved. The University of Minnesota is an equal opportunity educator and employer.