Welcome

Semi-Annual
Campus Merchant
Meeting
March 18, 2014
Meeting Agenda

• Team Introductions
• Risk Management- Herb Wagner
• Migrating to Secure Acceptance-Matt Stoner
• First Data Conversion
• PCI-DSS Compliance Validation Assessment
• PCI-DSS 3.0 Changes- New SAQ’s
• Bank of America- Brian Chapman
• P Card Compliance- Karen Brookbanks
• RegOnline Event Management Agreement
Maricopa Community Colleges notifies 2.5M after data security breach - Nov 27, 2013. Phoenix Business Journal

Target hacked: news and updates on the massive retail breach that affected millions – The Verge Jan. 16, 2014


Retail Breach Tied to Global Fraud Malware Hits Arizona Grocery Chain's Network- Arizona Daily Star February 2013

Woman admits stealing 15 IDs – Arizona Daily Star -August 29th, 2012

Gas stations at risk after 6 find devices to skim credit cards - Arizona Daily Star March 2, 2011
Never Forget—
We Are All In This Together!!!!!

- FSO-Bursar Department Services
- Information Security Office
- Internal Auditors
- Bank of America
- Campus Merchant
- Responsible People-
- IT Staff
- Risk Management
Risk Management Implications of Data Breach
Arizona Revised Statute §44-7501 – Notification of breach of security system; enforcement; civil penalty, preemption, exceptions; definitions

This is the primary Arizona law governing the response required when personal information is compromised through breach, data loss, or other compromise. Includes the following requirements:

• Conduct investigation to determine if breach has occurred
  • Breach = unauthorized acquisition of and access to unencrypted or un-redacted computerized data containing personal information
  • Personal Information = first name or first initial and last name in combination with one or more of the following: SSN, DL#, account number with PIN

• If breach is confirmed, must quickly notify affected individuals

• Attorney General may seek financial penalties of $10K/breach

• UA CIO required to make notification to ABOR

• UA typically offers 1 year of credit monitoring to affected individuals
Proper Management of Data Required by UA Policy
See: http://security.arizona.edu/ for guidance and policy information

The cost of compliance with mandatory notification requirements and follow-up monitoring can be significant, in private industry as much as $200/record. So a breach of just 5,000 unencrypted, un-redacted records could generate a response cost as high as $1,000,000.

Target Corporation – as many as 110 million compromised records. Target’s response costs were $61M in the fourth quarter alone. Costs to financial institutions have now exceeded $200M. Fraud is now showing up on 10-15% of stolen accounts. Total cost of breach expected to top $1B!

May become the largest single data breach loss in history.
For the University of Arizona – what is the risk?

• UA insurance from the State Risk Management program DOES NOT cover required corrective action, notification costs, or credit monitoring.

• UA Information Security Office and the CIO work with impacted units to minimize the cost of a breach, but….

• Net costs for breach response are the responsibility of the unit that suffered the breach.

• Cyber Liability insurance is available, but it is expensive and requires extensive documentation to purchase. Difficult to accomplish in a highly decentralized IT environment like the UA. For these reasons, the UA has not purchased cyber liability insurance.

• Don’t underestimate the reputational cost associated with a breach.
Strategies for prevention, and where to get help:

- Information Security Office in UITS - http://security.arizona.edu/

- Hire competent IT staff that understand security protocols, and know how to maintain properly patched servers and applications.

- Communicate a high priority commitment to data security from the highest levels of your unit. Don’t tolerate non-compliance.

- Educate your staff about UA security protocols, phishing and other schemes, hold people accountable for compliance.

- Report suspected data breaches to the ISO immediately. Waiting to report, or trying to hide the problem will make the problem worse and increase the cost impact.
Change Happens

- First Data
- PCI-DSS 3.0
- Secure Acceptance – Cybersource
- Assessment Tightening
Migrating Cybersource HOP to Secure Acceptance

Matt Stoner
Tips from success….
Getting started

- Test Business Center
  - Login password not the same as production
  - Most likely need to call Cybersource support and have reset
New Concepts

- **Secure Acceptance Profile**
  - Unique to each e-store
    - Profile ID will be on your new payment page
    - Key will be used by your web application
  - Payment acceptance settings need to be setup on the profile (previously on HOP settings)
New Concepts

CyberSource®
the power of payment

< All Profiles

The following settings determine your customer's checkout experience. NOTE: An active profile is read-only. To edit an active profile, return to the profile list and select edit.

General Settings
Profile name, ID, description, contact information, company name, and integration method: Web/Mobile or Stand Order Post.

Payment Settings
Payment types, accepted currencies, and authorization reversal.

Notifications
Merchant and customer notifications received after the checkout process is completed.

Customer Response Pages
The response page to display at the end of the checkout process based on the transaction result.

Security
A security key is required for all transactions, and for a profile to be activated.

Appearance and Branding
Customization of your checkout pages with your own company branding, including logos, color, and text.

Payment Form
The presentation of the checkout sections including the fields that are viewable, editable, or required.

Localization
View the list of CyberSource supported languages.
New Concept

- **SignedFieldNames**
  - Unique fields that you will choose to be required and part of the signature
Our Approach

- Replicated our current web application code with the prefix SA (secure acceptance)
- Code changes to the SA files while leaving the legacy code untouched, which provided a fallback option if something went wrong
Lessons Learned

- `bill_to_email` address is a required field (not documented as such)
- Testing profile can only have 1 payment card type, but production profile can have multiple
- Formatting amount 1000 not 1,000
- Double check your posted inputs and returned variable names/formats
Cybersource Resources

• Visit the Secure Acceptance Migration Center
To access documentation and other key migration information, please visit the Secure Acceptance Migration Center.
  – Webinars
  – Technical Resources
  – Assistance
  – FAQ’s
First Data Conversion Update

- We have completed conversion!
- Crediting back transactions on old platform
- Returning POS swipe terminals
- Clientline Access
“WHEN YOU CONSIDER THE METHODS USED BY ATTACKERS TO GAIN A FOOTHOLD IN ORGANIZATIONS—BRUTE FORCE, STOLEN CREDS, PHISHING, TAMPERING—IT’S REALLY NOT ALL THAT SURPRISING THAT NONE RECEIVE THE HIGHLY DIFFICULT RATING. WOULD YOU FIRE A GUIDED MISSILE AT AN UNLOCKED SCREEN DOOR? “

Verizon- 2013 Data Breach Investigations Report
“Will DSS 3.0 fix everything? The PCI SSC has stated that the changes in DSS 3.0 are designed to, “help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice.” The key themes are improving education and awareness, and increasing flexibility, and viewing security as a shared responsibility.” - Verizon 2014 PCI Compliance Report

• More to come as we clarify with the Council and our Assessors!
2013 Assessment Review

- Documentation
  - Incident Response
  - Policies
  - Training Doc’s
- Pan Scans
- Overall Department Understanding/Awareness
For Success-
We Must Move in the Same Direction

- It is a continuous circle – by protecting yourself, you are protecting the campus……
- Think Security not Compliance!
- Updates need to include all software components on a system, updated within minimum 30 days.
- Update Web pages/servers
- If you don’t need the data, don’t store it!
- Review procedures with staff
- Look for your own weaknesses and remedy and improve.
Bank of America

• Brian Chapman– Relationship Manager
Convenience Fees

**Visa**
**Points to Know:**
Convenience fee only assessed on Card Not Present
Amount of Convenience Fee only Fixed Amount
No Registration
No MCC limitations
Combine Convenience Fee with Transaction – Process as 1 Transaction
Same Amount of Convenience Fee assessed for All Payment Types

**MasterCard**
**Points to Know:**
• Service fee can be assessed on Card Present and Card Not Present
• Service fee can be assessed on PIN Debit and Credit Card
• Amount of Convenience Fee can be Flat, Percentage or Tiered based on Transaction Amount
• Can be different convenience fee amount for each payment channel
• Convenience fee on Debit can be different then on Credit, but must be the same amount on Card type
• Convenience fee cannot be higher than any other Card Based Payment
• Registration Required
• Only these MCC Codes are allowed to assess Convenience Fee 8211, 8220, 9211, 9222, 9311, 9399
Can be processed as 1 transaction but best practice is to complete as 2 separate transactions

**AMEX**
**Points to Know**
Convenience fee is assessed in same manner as other card types
Convenience fee cannot be different across payment types
Amount of convenience fee can be Flat, Percentage, Tiered based on Transaction
Can be processed as 1 transaction but best practice is to complete as 2 separate transactions
**Discover**

**Points to Know**
- Convenience fee is assessed in same manner as other card types
- Convenience fee cannot be different across payment types
- Amount of convenience fee can be Flat, Percentage, Tiered based on Transaction
- Can be processed as 1 transaction but best practice is to complete as 2 separate transactions

**Government and Education Payment Program**

**Visa**

**Points to Know:**
- Service fee can be assessed on Card Present and Card Not Present
- Service fee can be assessed on PIN Debit and Credit Card
- Amount of Service Fee is Variable Amount
- Can be different variable amount across payment channels
- Can be different variable amount for each payment type
- Registration Required
- Merchant Verification Value Assigned
- Only these MCC Codes are allowed to assess Service Fee
  - 9311, 8244, 8249, 8220, 9211, 9222, 9399
- Must be processed as 2 separate transactions. (sale) and (DBA name*service fee)

**Surcharge**

In November 2012, the United States District Court for the Eastern District of New York preliminarily approved a proposed settlement agreement in the Payment Card Interchange Fee and Merchant Discount Antitrust Litigation. As part of this settlement, Visa and MasterCard will be implementing rule changes, effective January 27, 2013, which will include the ability for merchants in the US and US territories to surcharge certain Visa and MasterCard credit card transactions.
EMV Mandates Summary

- Equipment
  - New Equipment
  - May have some compliance PCI validation changes

- Cards- New cards issued to customers

- Liability Shift- Oct- 1, 2015
PCard Administration

Karen Brookbanks
Procurement & Contracting
PCard Administrator
621.3288
kbrook@email.arizona.edu
RegOnline Event Management

REGONLINE—THE COMPLETE EVENT-PLANNING SOLUTION

• Master Service Agreement University of Arizona Pricing
• Per Registration Fee: $2.84
• Credit Card Processing using the RegOnline Gateway: 2.75%
• No set up costs
• Event is sent a paper check once a week net of fees
• Online reports
• Personal Account Manager- Jen.Gaffney@activenetwork.com
• Minimum PCI footprint/requirements

Contact Robbyn Lennon to provide application and to set up account.
News/ Changes & Not So Subtle Reminders.

- Bank of America/Clientline account access
- American Express and Discover access
- Account changes and questions- Contact FSO-cashandclearing@email.arizona.edu
- Reconciling- Please reconcile at a minimum monthly!!
“When we share a common direction and a sense of community, we can get where we are going more quickly and easily because we are traveling on each others energy and power. “
Questions & Assistance
Email  FSO-Bursar Department Services-
Merchants@fso.arizona.edu or
Contact Robbyn Lennon
621-5781,
rlennon@email.arizona.edu