Financial Management Meeting

**Agenda**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30 a.m.</td>
<td>Welcome &amp; Introductions</td>
<td></td>
</tr>
<tr>
<td>9:35 a.m.</td>
<td>Business Services Updates</td>
<td>Martha Kerner (5 minutes)</td>
</tr>
<tr>
<td></td>
<td>● Internal Controls Update</td>
<td></td>
</tr>
<tr>
<td>9:40 a.m.</td>
<td>Risk Management Updates</td>
<td>Rick Gibbs (10 minutes)</td>
</tr>
<tr>
<td></td>
<td>● Introduction of International Risk Manager</td>
<td></td>
</tr>
<tr>
<td>9:50 a.m.</td>
<td>Accounting Services Updates</td>
<td>José Carus, Dan Langer and Carla Raatz (10 minutes)</td>
</tr>
<tr>
<td></td>
<td>● Non-resident Alien Scholarships</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Funding Delays in DP/PIR Procession</td>
<td>Rusty Haines (5 minutes)</td>
</tr>
<tr>
<td>10:05 a.m.</td>
<td>Purchasing Services Updates</td>
<td>Hartley Murray (15 minutes)</td>
</tr>
<tr>
<td></td>
<td>● Purchasing Fraud</td>
<td></td>
</tr>
<tr>
<td>10:20 a.m.</td>
<td>Other Q&amp;A</td>
<td></td>
</tr>
<tr>
<td>10:30 a.m.</td>
<td>Adjourn</td>
<td></td>
</tr>
</tbody>
</table>
Business Services
Non-Resident Alien Scholarships

• Any payments made through payroll effective January 1, 2015

• Applies to lump-sum payments for all registered students

• New earnings and account code setup
  – Earnings Code SF5
  – Account Code 5714; will be automatically assigned based on earning code

• No fringes will be taken
PURCHASE ORDER SCAM

Targeting U.S. Companies
& Universities
Credit for the content:

This PowerPoint provided originally by FBI, edited by Purchasing Services
SA Joanne Altenburg – Washington Field Office
SSA Paula L. Ebersole – Washington Field Office
Objective of the Scam:

• To use university and corporate identities to obtain merchandise on credit

• To export the merchandise before the victim vendor discovers the fraud

• Operating primarily from Nigeria, outside U.S. jurisdiction
Items Being Purchased:

- Computers & Related Equipment
- Projectors/Cameras
- Card Printers, Stock & Ribbons
- Pharmaceutical Equipment
- Industrial Equipment
How the Scam Works:

- Imposter domain and VoIP phone numbers are established
- Establish US address to receive and re-ship products

Email & fraudulent Purchase Orders sent to US **vendors** – net 30 day credit

**Vendor** ships products to US address (re-shipper)

**Vendor** bills impersonated company or **university**

Merchandise received at US address (re-shipper)

**US Freight Forwarder** ships to Nigeria, often through the UK

**Victim**
Step 1: Bad guy establishes domain names similar to an established business/university

Real Entity: University of Michigan

www.umich.edu

Fraudulent Domain Names and Email Accounts:

Purchasing@umichsregentstores.com
Purchasing@umichedu.us
Purchasing@umiredu.com
Purchasing@umichedu.net
Purchasing@umichregentsedu.com
Purchasing@umregentsedu.com
**Step 2:** Bad guy establishes phone numbers which appear to be associated with the impersonated entity

- Use of Voice Over IP phone numbers with U.S. **local area codes**
Step 3: Bad guy establishes U.S. addresses to receive and re-ship products

- Using dating sites or ‘work from home’ ads on Craig’s list

Profile of Re-Shipper:
- Addresses are residential
- Generally lower income
- Lonely hearts victims
- Workers at self storage facility

- Establishing a self-storage unit or account with a warehouse facility
Self-Storage or Warehouse

• The storage unit is opened using the identify of a legitimate company, with copies of a fabricated drivers license and if payments are made, stolen credit cards are used

• Midnite Express – a real freight company in North Dakota
Step 4: Bad guy requests product quotes using email accounts on bogus domains

- **Name:** Mike Hardiman
- **Phone:** 608-268-9385
- **Email:** purchase@uwmedu.us
- **Questions/Comments:** Hello, I would like to know if you carry the below items, kindly provide us a pricing on the items if you do. Fluke Clamp Meter 376 Fluke 87-v digital multimeter
- **Warm Regards**
- **Director of Purchasing Services Mike Hardiman**
- **University of Wisconsin-Madison**
- **Tel:** 608-268-9385 Fax:608-268-895
Step 5: Bad guy emails Purchase Orders on fabricated letterhead

To be shipped to an address where the packages will be accepted and re-shipped

To be billed to the real company on 30 day credit terms
5235 Merriman Rd Westland MI

U-HAUL  Your moving and storage resource.

Mr Stor It (U-Haul Neighborhood Dealer)

Address
5235 Merriman Rd
Westland, MI 48186
(734) 729-3165

(N Of Detroit Metro Airport)
Driving directions

View photos

View website

★★★★★ 3 reviews
Step 6: Bad guy obtains tracking information from the victim company to determine if/when the packages are delivered (we’ll come back to this)

-----Original Message-----
From: John Smith@abc-products.com
Sent: Wednesday, March , 2014 10:23 AM
To: Sales@ Computer_Supplier.com
Subject: Re: Urgent reply

Kevin, how are you doing? I just wanted to touch base to see if the 20 Units has been shipped. Do keep me updated on the ETA details.

Thank you
    John
Step 7: Bad guy arranges reshipment, generally sending shipping labels to the re-shipper

From: "Brian Haegen" <brianhaegen@yahoo.com>
Date: Jan 9, 2013 10:17 AM
Subject: FedEx labels 1 - 10
To: 2love02@gmail.com" <2love02@gmail.com>

Honey,

Find attached FedEx labels 1 to 10. Print out pages 1 to 10 and tape a page on each of the boxes. Each box will have a FedEx label on it. Do ensure labels are well taped so that they wont come off while boxes are in transit, also ensure you can read each label after taping.

Love you,
Brian
Step 8: Goods are shipped to a freight forwarder using the labels provided.
Use of Stolen DHL Accounts:

• Re-shippers are provided with DHL Labels
• The labels utilize stolen DHL accounts
• The merchandise is shipped to the United Kingdom to be re-shipped
Step 9: Victim vendor bills the university or company being impersonated

```
<table>
<thead>
<tr>
<th>Price ea.</th>
<th>Subtotal</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2,990</td>
<td>$59,800.00</td>
</tr>
</tbody>
</table>
```

```
Remit to:
Computer Supplier, Inc
129 First St
Las Vegas, NV

800-948-9566 Fax: 800-948-9532

Please return one copy with payment

1.5% MONTHLY FINANCE FEE WILL BE BILLED ON ALL INVOICES PAST TERMS.

Customer PO: 149636

Bill To:
ABC Products Inc
725 Main St
Alexandria, VA 22010

Date: 3/30/2014
Invoice No: 47615
```

Total Due: $59,946.82
Payment terms: 30 days

Thank you!
• The vendor doesn’t learn of the fraud until the real university or company receives the invoice and notifies the vendor that they have been scammed

• The goods are generally out of the country within a matter of days
Latest Variation (worrisome):

• Vendors ship to an address associated with the university or company being impersonated
• Bad guy requests the package be re-routed or held to be picked up at a FedEx or UPS facility

Location associated with impersonated school or business

Goods are re-routed to be picked up and reshipped
Indicators of Fraud:

• Incorrect domain name on email and POs
  – Variation on the company/university true domain
  – University domain names that do not end in .edu
    (we’re seeing xxxxxedu.us)

• Gmail or Yahoo email addresses used
  • abc.co@gmail.com

• Shipping address is not the same as the business location

• The delivery address is a residence or self-storage facility
Indicators of Fraud:

- Poorly written email with grammatical errors
- Phone numbers not associated with the company/university
- Unusually large quantities are requested
- Rush to ship priority/overnight
- Ship to address typically outside of Wisconsin
What are we doing:

• Keeping all records in their original form
• Forwarding info to UW Police and our FBI contact.
• Not advising vendors what to do other than:
  – FBI recommends you not communicate with criminals
  – Contact their local authority
  – Contact their local FBI office
  – Point them to the FBI website www.ic3.gov
Our message to vendors:

Purchasing Services
Division of Business Services

Purchasing Services

Purchasing provides the University with effective and responsive life cycle procurement practices. See our Mission and Vision for more information.

Items of Interest

- Notice to Suppliers: Fraudulent Purchase Order Email Activity
  We want to alert you to an active email scam involving purchase orders and request for product quotations that claim to originate from the University of Wisconsin but are in fact fraudulent. More information is available in the full notice.
  (added 5/16/14)
Our message to vendors

http://www.bussvc.wisc.edu/purch/VendorInfo/fraud.html

Notice to Suppliers: Fraudulent Purchase Order Email Activity

We want to alert you to an active email scam involving purchase orders and request for product quotations that claim to originate from the University of Wisconsin-Madison but are in fact fraudulent. While the university cannot prevent this illegal activity, we are actively working with law enforcement to investigate these fraudulent email contacts.

We can share some common traits or themes of these fraudulent emails that may help reduce risk to your company in becoming a financial victim of this scam:

- The email message is poorly written, with misspellings and awkward sentence structure
- The sender's email address or website link are not authentic to the University of Wisconsin-Madison
- The message requests shipment of products to non-University of Wisconsin-Madison addresses
- The message may include an attachment that is designed to look like a purchase order, may include a logo or other graphic, and a signature that may look legitimate

If you believe you have received a fraudulent email that appears to be from the University of Wisconsin-Madison, you may forward it to our Purchasing Services department at purch@bussvc.wisc.edu to verify its legitimacy before responding to the email or filling the order. You may also contact the Purchasing Services department by phone, Monday through Friday, 7:45 am to 4:30 pm at (608) 262-1526.

Purchasing Services and the University of Wisconsin-Madison value our partnership with you and appreciate the very important role you play in providing goods and services to our faculty, students and staff in support of their academic, research, and patient care endeavors. Please know that we are assisting to the fullest extent we are able with the investigation of this illegal activity by reporting all fraudulent emails to appropriate authorities.
What should **you** be aware of:

- Think twice before giving out your name or that of any purchasing agent or department person. Perform some due diligence as to who is asking for it and where possible redirect caller to that department’s central number.
- Don’t point questionable callers to our staff directories.
- Don’t answer e-mails like this:

```
IT-Service Help Desk
Nicole King <nicole.king@rentonschools.us>
Sent: Mon 10/13/2014 7:06 AM
To: info@my-mail.org

Please **Click Here** to Validate your email account
```
Caller ID info:

- Check your inbound caller ID or URL’s for foreign inbound calls from Nigeria
Questions?
Future Financial Management Meetings
Rooms 1106 & 1108, 21 N Park Street
9:30-11:30AM

2014
December 9