OPCS Overview

The implementation of the Ohio Pooled Collateral System creates a unique partnership between:

- Treasurer’s Office
- Financial Institutions
- Local Governments
OPCS Overview

- The Ohio Pooled Collateral System allows for participating Financial Institutions (FI) to pool collateral for Ohio Public Unit’s (PU) deposits.

- The Treasurer of State (TOS) is the sole administrator and monitor of the program.

- FI’s will chose to 1) participate in the pooling method (OPCS) collateralizing at 102% or a rate set by the Treasurer’s Office in rule or 2) not participate in OPCS and collateralize all public entities with specific pledge method at 105%.

Benefits of OPCS

- Centralized collateral monitoring will save time and resources for local governments by shifting the administrative burden for managing pledged collateral to the Treasurer’s Office.

- Provides administrative benefits for financial institutions by streamlining the processing and management of pledged collateral.

- Guards against fraud since the TOS will be able to see all pledged collateral compared to the total amount of public deposits at a financial institution.

- OPCS does not impact a local governments ability to select which eligible institution will hold its deposits.
Public Unit Responsibilities

• Public Units will Participate in OPCS Using the Following Methods:
  • The Treasurer of State will provide market pricing of all collateral and publish the reports on the OPCS portal.
    • Public Units will be responsible for reviewing and monitoring the reports posted, verifying the accuracy of reports of their itemized deposits, and reporting any discrepancies to their financial institution.
  • The Treasurer of State will provide OPCS access to the public units.
  • Public units shall periodically certify account details, including deposit balances, and contact details are correct, in accordance with the schedule set by the Treasurer of State.
  • Public Units may negotiate a public unit negotiated collateral requirement for individual accounts with their financial institution, which may be higher than the statutory collateral requirement or the reduced collateral floor as applicable.

Why OPCS?
OPCS Home Page

This dashboard will allow you to see if your financial institution has submitted their files on time to TOS.

OPCS Dashboards

This dashboard will display collateral sufficiency information for your Local Government. The information on the dashboards can be exported to excel.
OPCS Dashboards

- View Details

Public Unit Dashboard

File Receipt Dashboard
- Depositing Information & Sufficiency Dashboard

- Next Sufficiently Collateralized
- Under TOS Cushion
- Sufficiently Collateralized

Drill down tools: Search Public Units > 11111111 > File/Track 12/30/2017 > MyBook > POOL_MAN > City

- Export to Excel

<table>
<thead>
<tr>
<th>Account num.</th>
<th>Account line 1 for Acc. 1</th>
<th>Account line 2 for Acc. 2</th>
<th>Principal</th>
<th>Accrued Int.</th>
<th>Balance</th>
<th>Proxy SDL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DDA</td>
<td></td>
<td>$0.00</td>
<td>$0.00</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$2,000,000.00</td>
<td>$0.00</td>
<td>$2,000,000.00</td>
<td>$250,000.00</td>
</tr>
</tbody>
</table>

1, 2 of 2 items

SCALE

opcs.ohio.gov
Model Objectives

The Treasurer’s Office used the following objectives when drafting the Model:

- Be stringent, but fair
- Be transparent, objective, and externally reproducible – be predictable
- Only use data for evaluation from externally and publically available sources, no additional data requested from FIs
- Evaluate a FI’s micro-economic condition, as well as its relative position to Ohio, regional, and national peer groups
- Evaluate and take into account macro-economic issues indicators
- Recognize and risk account when external market data elements are unavailable for a FI

SCALE Components

Sensitivity to Risk is the degree to which changes in interest rates, foreign exchange rates, commodity prices, or equity prices can adversely affect a bank’s earnings or economic capital.

Capital Adequacy is a measurement of a bank to determine if solvency can be maintained due to risks that have been incurred as a course of business.

Asset Quality evaluates risk, controllability, adequacy of loan loss reserves, and acceptable earnings; and the effect of off-balance sheet earnings and loss.

Liquidity is what a bank requires if funding is interrupted and the bank must still be able to meet certain obligations, i.e. the bank’s ability to repay depositors and other creditors without incurring excessive costs.

Earnings determine the ability of a bank to increase capital (through retained earnings), absorb loan losses, support the future growth of assets, and provide a return to investors.
Questions

Lizz Lewis, Director of Legislative, Policy & Constituent Affairs
Elizabeth.Lewis@tos.ohio.gov – 614-728-9251

Thank You!
Types of Fraud


Samples of Fraud

Tools to ID Fraud

Legislation to Address
Four types of risk to watch for in all daily operations

- Check
- ACH/Wire
- Card
- Cyber

Four areas we’ll discuss today

✓ Statistics
✓ How can you detect fraud
✓ Visual samples
✓ How can you mitigate the risk of fraud

payment fraud affected

2016 73% of organizations with typical loss of $20,000*

2016 AFP Payments Fraud and Control Survey; * 2015 AFP Payments Fraud and Control Survey
ACTUAL OR ATTEMPTED FRAUD STATISTICS

71% Check Fraud

39% Card Fraud

48% Wire Fraud

25% ACH / Debit Fraud

2016 AFP Payments Fraud and Control Survey

2013 Federal Reserve Payments Survey

2015 Wire Fraud Stats - Internet Crime Complaint Center (IC3) Business E-mail Compromise.htm
✓ 91% of successful data breaches started with a spear phishing attack.

✓ Ransomware was a 1 Billion dollar criminal business in 2016 and continues to grow. There was a 752% increase in new ransomware families in 2016. Less than half that paid the ransom (45%) got their information back.

✓ CEO Fraud (aka Business Email Compromise) causes $5.3 billion in damages.

✓ Recent studies show that over 54% of users click on a phishing link in under 60 minutes
  ✓ Average cost per record of a data breach is $221 in the US
  ✓ Average cost per incident of a data breach is $7 million in the US

Information from IBM/Ponemon Institute 2016 Study
Check Fraud

✓ Altered dollar amount
✓ Forgery
✓ Stolen or reprinted stock

ACH/Wire
25% of organizations were subject to at least one ACH fraud attempt in 2015 resulting in financial loss

- Share rises to 26% among large organizations with more than 100 accounts
- Reasons why the organization was financially responsible for the losses sustained from the ACH fraud include:
  - Not reconciling accounts on a timely basis
  - Not using ACH debit blocks or ACH debit filters and ACH Positive Pay
  - ACH return not being timely

### Frequency of Attempted or Actual ACH Fraud

<table>
<thead>
<tr>
<th># of ACH Fraud Attempts</th>
<th>All Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 5</td>
<td>72%</td>
</tr>
<tr>
<td>6 to 10</td>
<td>13%</td>
</tr>
<tr>
<td>11 to 20</td>
<td>5%</td>
</tr>
<tr>
<td>16-20</td>
<td>2%</td>
</tr>
<tr>
<td>21 or more</td>
<td>9%</td>
</tr>
</tbody>
</table>

RECENT WIRE FRAUD SCAM

**Business E-Mail Compromise**

- Growing number of email accounts of authorized officers within corporate companies are compromised by fraudsters - called Masquerading
- The fraudster takes over an executive’s email or uses a “spoofed” email that appears to be from the executive.
- The fraudster, posing as the executive, emails lower level employees instructing them to send a wire or ACH.
- The employees receiving the request do not question the email and have the wire or ACH imitated (usually internationally).

**Mitigation Strategies**

- Instituting maximum online security including strong authentication practices on your email and your entire network to mitigate this fraud.
- Do not rely on written email payment orders or faxed payment order requests as your approval as authorization to execute your wires, instead call your Sr. Managers to confirm.
Re: Request

David MacKinnon

Sent: Wednesday, September 16, 2015 at 4:47 PM
To: Rohyt Belani
Cc: Samuel Hahn

Rohyt,
I'll get this done ASAP. Do you want the funds in dollars or GBP?
Thanks,
Dave

Sent from my iPhone

On Sep 16, 2015, at 4:41 PM, Rohyt Belani <rohyt.belani@ahshme.com> wrote:

The details are below. Let me know once it has been processed.

Bank Name : Raytown-Lee's Summit Community Credit Union
Bank Address : 10021 E 66th Ter, Raytown, MO 64133
Bank phone number : 816-356-1452
Name On Account : Robert Lee Koerner
Account Number : 201258
Routing Number : 221300016
Home Address : 6553 Raytown Rd, Apt 1B, Raytown, MO 64133
Amount : $29,000

Thanks
Sent from my iPhone
**Action Steps**

- Clear Logins and Passwords, especially if using a public computer
- Be alert for phishing—always verify a site is secure (indicated by https://) when entering card info
- Verify your address with both the Post Office and your financial institution; notify card companies prior to a change in address
- Utilize authorization controls to restrict purchases
- Monitor transaction activity on an ongoing basis
- Reconcile accounts on a regular basis—monthly

**Things to Avoid**

- Avoid leaving your card(s) unattended at work—more credit card thefts occur in the workplace than anywhere else
- Avoid giving your card number over the phone whenever possible; only give it when you have initiated the call and need to place an order
- Do not leave your card in a vehicle—loose cash and cards are easy targets
- Avoid signing a blank receipts (or leaving any line incomplete)—most often occurs at restaurants or bars

**Set specific authorization parameters including:**

- **Corporate Credit Limit** - Determines the maximum amount that may be spent through combined purchasing activity of all cardholders in the organization.
- **Cardholder Credit Limit** - Determines the total purchasing activity available per cardholder or card.
- **Dollars per Transaction** - Restricts the maximum dollar amount of any purchase made.
- **Dollars and Transactions Limit** - Establishes the maximum dollar amount or number of transactions that will be authorized each specified period (i.e., day, month, cycle, year).
- **Merchant Category Codes (MCC)** - Enables your organization to restrict use of card at specific categories of business
✓ Urgency to click on a link to update or verify account information and often mention negative consequences for failing to respond.
✓ Unexpected and may be inconsistent with other emails from the company.
✓ Sometimes contain spelling errors and bad grammar.
✓ May come from a company with whom you do not currently do business.
✓ Ask for information they should already know or shouldn’t need to know.
✓ Contain a link in the email that you are urged to click and when you hover over that link, it does not appear to be related to the company sending the message.
✓ Includes an attachment you are urged to open or download.
From: Google [mailto:sales@crazearmarketing.com]
Sent: Wednesday, February 24, 2016 6:34 PM
Subject: IMPORTANT Security Reminder

Account User,

We’ve detected that your email notifications and account recovery is no longer active because security preferences settings is currently set to Manual Mode. Security preferences settings has to be reset to ‘Automatic’ (Recommended) to re-activate all notifications and recovery to help secure your email. It also enables recommended updates be downloaded and installed automatically.

To review settings, kindly see ‘Security Preferences’ now.

We advise that you complete to help secure your account.

Best,
Google Accounts Team

This email has been sent from a virus-free computer protected by Avast.
www.avast.com

From: 'FifthThird@ndst59.com'
Date: Tue, Feb 16, 2016 at 1:57 PM
Subject: 53rd: Account Notice For Issue ID#4521
To:

Dear Fifth Third Online1st Customer:

We’re writing to let you know that there is restriction on your account, due to unusual activities on your account.

To remove this restriction kindly log on to www.53.com/rec-802/ and update your Account profile.

If you aren’t enrolled to receive Paperless Statements and Notices or you think you’ve received this message in error please disregard the message.

This email can’t receive replies.

© 2015 Fifth Third Online, N.A. Member FDIC
How can I tell if my computer has spyware running on it?

By design, spyware is difficult to detect, but here are some things you may notice:

- Additional toolbars added to your web browser that you did not authorize.
- Pop-up windows that advertise services that you did not request.
- Unusual “windows” that show up and possibly go away when you start your computer or are browsing the Internet.
- Unusual links showing up in web pages where there are not usually links. These links will probably lead to web pages advertising some service.
- An unusual slow down in your computer’s performance.
- The appearance of unexpected programs in your computer’s startup folder.
Current Legislation - Ohio

✓ House Bill 312 - Commercial Card / Purchasing Cards
  ✓ Requires controls and policies
  ✓ Best Practices
✓ ORC 135.185 Ohio Collateral Reform

Thank You
For Your Time

Questions?