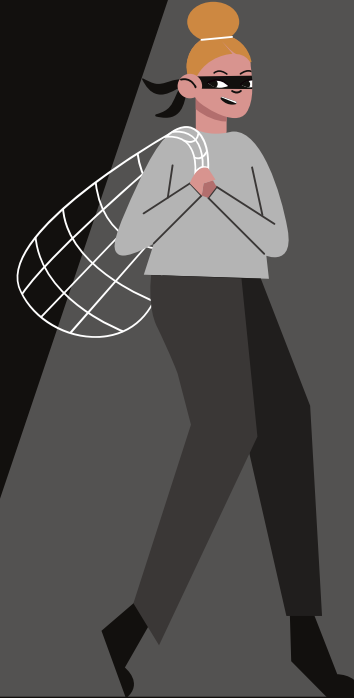


PREVENTING FRAUD

A PANEL DISCUSSION

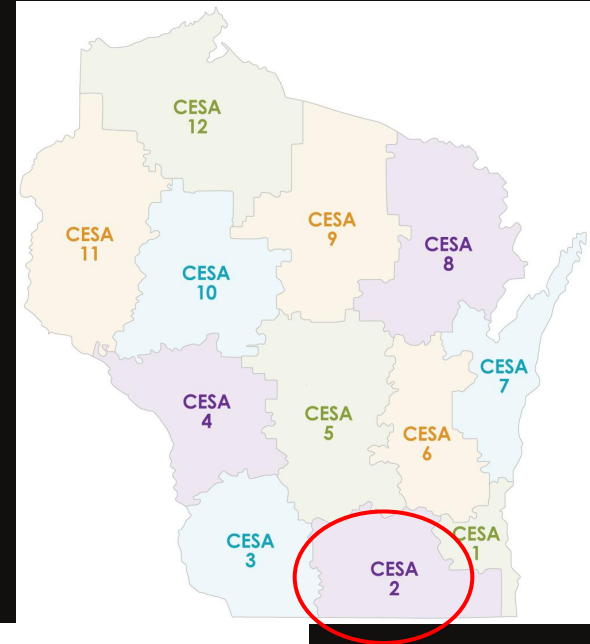
Jason Demerath, CESA 2
Wayde Pollock, CESA 4
Hilary Cordova, CESA 9



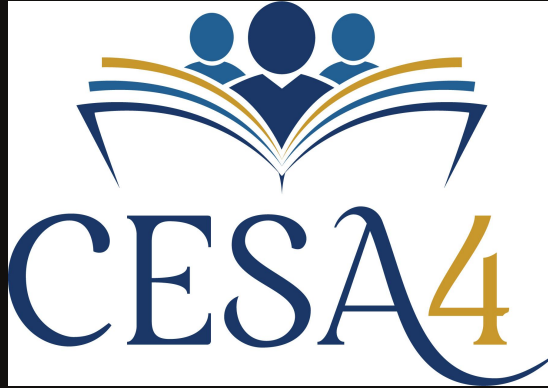
Meet the Panel



JASON P. DEMERATH, CSRM, SFO
Executive Director of Financial Services

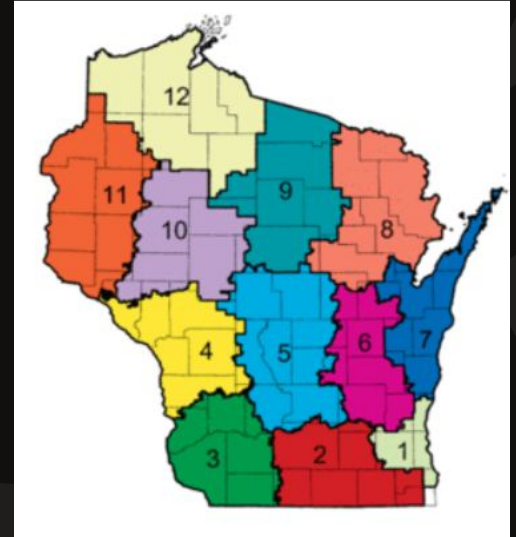


Meet the Panel



WAYDE POLLOCK

Director of Finance & Former Governmental Auditor



Meet the Panel



HILARY CORDOVA
Executive Director of Business Services



Fraud via Email

Transfer Fund



Inbox x



? Nordine, Dawn <dnordine@cesa9.org>

11:11 AM (21 hours ago) ☆

Reply ▾

to me ▾

Hello Hilary,

I want you to handle this today as i will be attending meetings and its imperative the payment goes out today.

can you make a wire transfer of \$ 13,860 to a vendor,which is for purchases as well as program services and public relations services fees all supporting documents will be forwarded to you before the end of today.I'm in a meeting right now,we can only communicate by mail now,i will just keep an eye on my mail for your reply.

Let me know if you can get on this today so i can forward the beneficiary details Immediately.

Kind Regards,

Dawn

Fraud via Email

- From a “legit” employee email

But...

- Vague information
- Lack of capitalization
- Incorrect punctuation
- Poor grammar
- Just doesn't seem right




Fraud via Example

Elizabeth Sanger-Kuckkan <esanger-kuckkan@cesa9.org>
to me ▾

Hi Ryan Kottke,

Can you please assist me with changing of my direct deposit info before the next payroll?

Regards
Elizabeth Sanger-Kuckkan

 Virus-free www.avg.com



Fraud via Email

- From a “legit” employee email & domain address
- No typos
- Correct grammar
- Nothing out of the ordinary

Skyward

Careful line-by-line review of your Payroll ACH file before every payroll is an essential internal control.
Please be vigilant in monitoring your ACH.

Careful line-by-line review of your Payroll ACH file before every payroll is an essential internal control.
Please be vigilant in monitoring your ACH.

[EDUCATION](#) | [RESOURCES](#) | [CAREERS](#) | [CALENDAR](#) | [WASBO GO](#) | [CONNECTWORK](#)

Hello WASBO Members:

WASBO colleagues are reporting hackers fraudulently changing employees' bank accounts. Hackers are reportedly targeting payroll ACH and disabling bank change notifications so districts don't see the scam unless they physically look at the ACH file very carefully.

Everyone should be checking their payroll ACH and looking for any changes to banks. Fraudulent banks that have been reported are Green Dot Bank, Pathward Bank, GoToBank, and The BanCorp Bank. There could be more.

Careful line-by-line review of your Payroll ACH file before every payroll is an essential internal control. Please be vigilant in monitoring your ACH.



Wisconsin Association of School Business Officials

4797 Hayes Road, Suite 202 | Madison, WI 53704 | P 608.249.8588 | F 608.249.3163

www.wasbo.com

If you no longer wish to see emails related to this topic, please [update your WASBO communication preferences](#).
If you no longer wish to receive any emails from WASBO, please [unsubscribe](#).

- Phishing Email
- Access to Skyward
- Change in Bank Information for Payroll ACH
- Emails Filtered Before Seen

Skyward

The bad actors are using business email compromise (bec) to gain access to a user's email, and from there use the forgotten password feature (if turned on by the district) to reset the password for the user's Skyward login. This is why it is critical to use multi-factor authentication (MFA) and turn off the ability to reset a password via email for any user with access to sensitive information and especially for super users.

Once logged in the bad actor makes changes to ACH information. In the situation where the ACH account changed is for the user whose email they compromised, the bad actor sets up an email rule on the user's email account to delete the ACH change email. That way the user whose email was compromised never sees the change to their ACH account happened.

Skyward

3. RE: Fraud Warning: Payroll Scams Hitting Districts



[Cassandra Shearer](#)

Actions ▾

Posted 2 days ago |  [view attached](#)

I reached out to skyward and they had some good tips.

Attached is their response which includes

The importance of 2 factor authentication

Setting up an email alert for any banking changes for payroll as well as AP.

There is a report you can run that will list any banking changes for payroll. [Skyward Report Instructions](#)

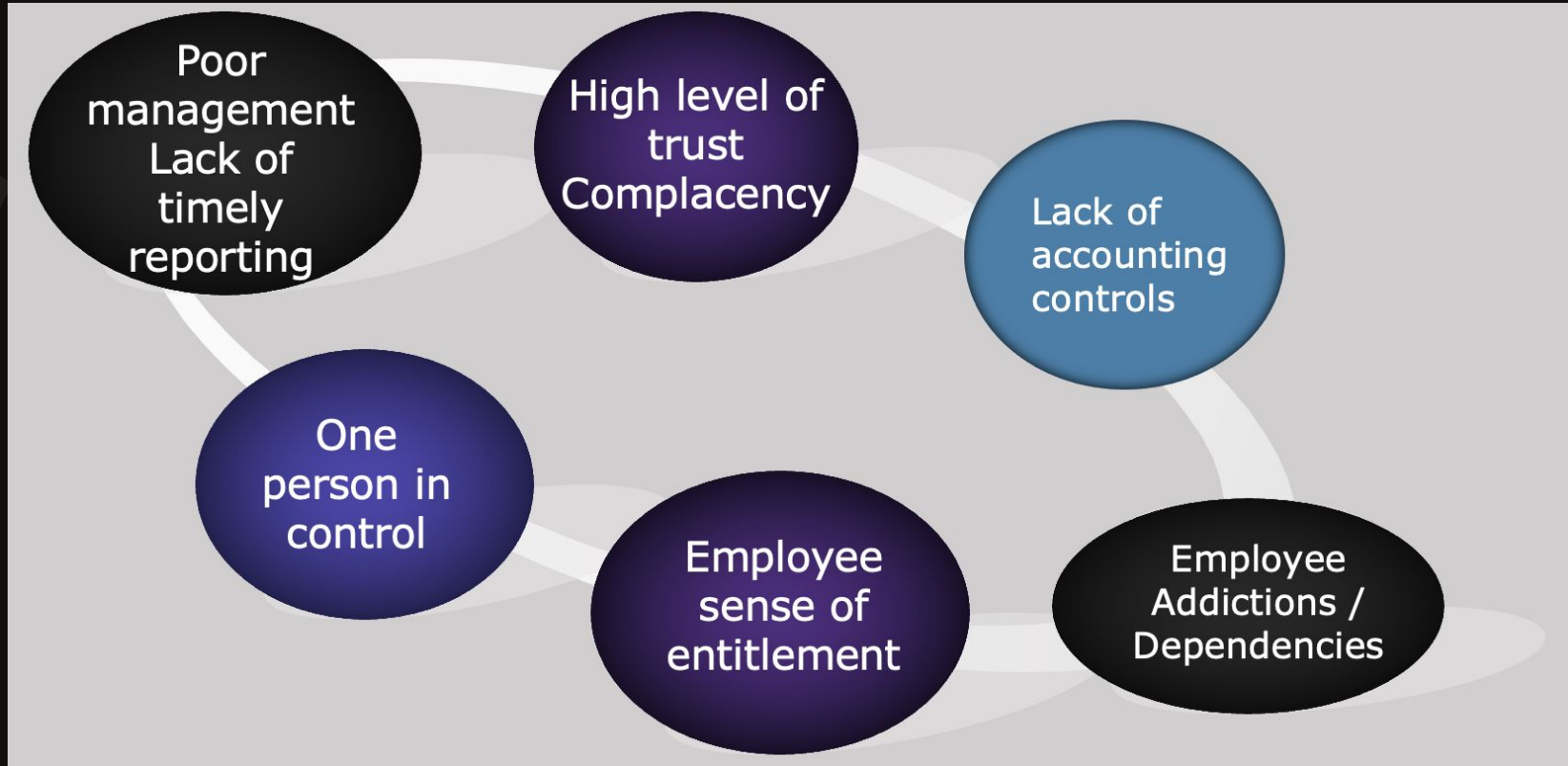
On another note, we had some fraudulent checks try and get through and so we set up positive pay on all our accounts.

Good luck!

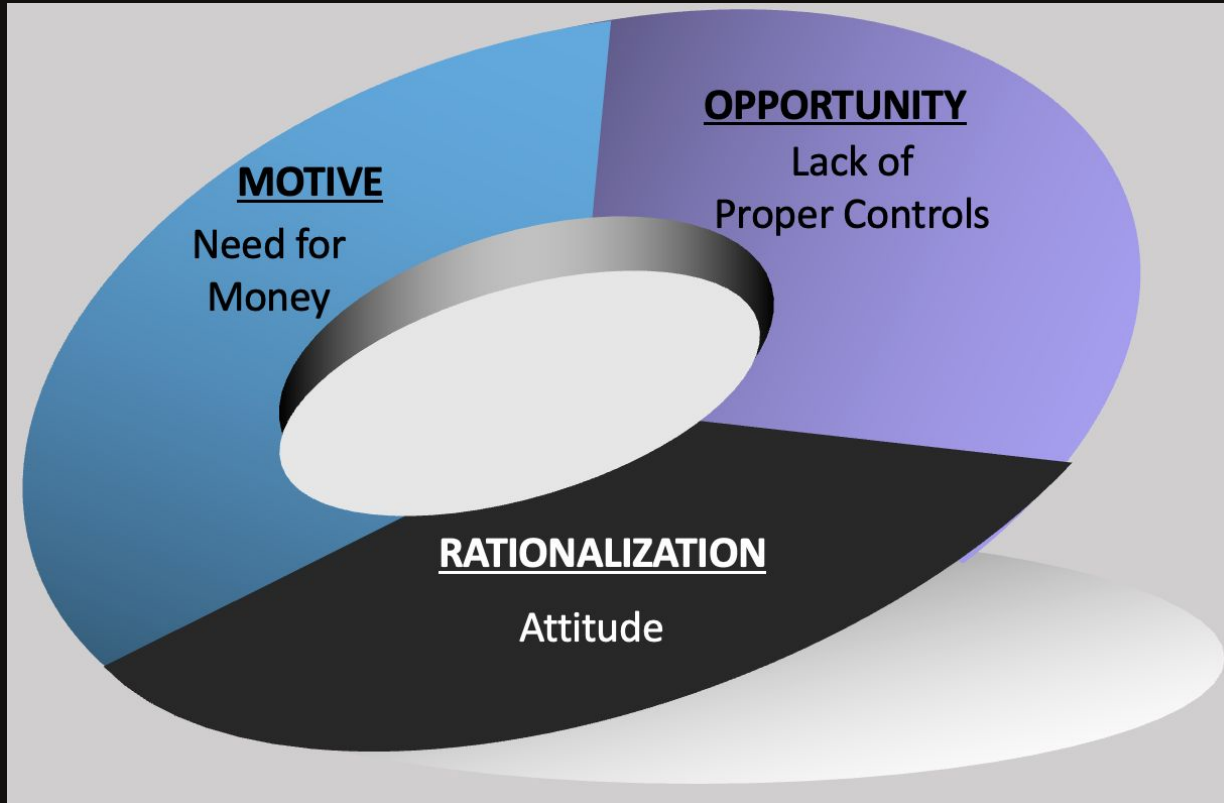
True Example of Internal Fraud

- Details on the Discovery of Embezzlement
- Clues Pointing toward possible cover up
 - Lack of taking multiple days of vacation
 - Working additionally before & after hours
 - Providing prepared spreadsheets for documentation
 - Not letting others assist with the person's work

Why Does Most Internal Fraud Occur?



Formula for Internal Fraud



Activity Accounts

- High Risk Area
- Individuals Not Financially Trained & Very Busy
- Lots of Cash Handled
- Cash Accepted by Teachers/Advisors/Students
- Concession Stand Fundraisers & Athletic Ticket Sales
- Not Necessarily Linked to District Financial Software
- Lack of Advanced Planning = Need for Funds Quickly
(i.e. leaving on a trip, taking group to an event, etc.)

Internal Controls

- Most common audit finding “Lack of Segregation of Duties”
- How do you minimize it or even eliminate it
 - Cash Deposit Duties
 - Cash Disbursement Duties
 - Journal Entries Duties

Cash Deposit Duties

Who opens the mail?

Who prepares the deposit?

Who takes the deposit to the bank?

Who enters it into the general ledger?

Who reviews it / approves it?

Who batch updates to the general ledger?

Cash Disbursement Duties

Who opens the mail?

Who distributes the invoices for coding?

Who reviews the coding of the invoices?

Who enters it into the general ledger?

Who reviews it / approves it?

Who batch updates to the general ledger?

Journal Entries Duties

Who initiates the journal entries?

Who reviews the journal entries to be prepared?

Who enters it into the general ledger?

Who reviews it / approves it?

Who batch updates to the general ledger?

Verification for EVERY ACH Change

- Must talk to an authorized person regarding the request & document it
 - For employees
 - (1) Contact
 - In person (noted)
 - On the phone
 - Must call the phone number on file in Skyward, NOT one provided in the request
 - (2) Verify Account
 - Require a copy of a check
 - Or a prenote
 - For vendors
 - (1) Contact
 - Must call the phone number on file in Skyward, NOT one provided in the request
 - (2) Verify
 - Prenote required

Fraud via Email

ISCorp: We have recently changed our Remittance address and ACH information External ISCORP x



Accounts Receivable <accountsreceivable@iscorp.com>
to me ▾

Wed, Dec 28, 2022, 12:25 PM ☆ ↶ Reply ⋮

Dear Cesa 9,

We at ISCorp have changed our remittance address and ask you kindly to update your accounting records to pay to

ISCorp
PO Box 75278
Chicago IL 60675-5278

going forward. We do still accept check, but ACH is much preferred. The new routing information is on all invoices since February of 2022 and I have our new banking information in the PDF attached to this email as well.

Please respond too ensure that this email won't be sent again.

Thank you in advance,
ISCorp Accounting



Accounts Receivable
Finance and Billing
Main: (262) 240-7777
Direct: (262) 240-7777 Option 3
www.iscorp.com | [in](#)

"ISCorp, Proprietary & Confidential"

This e-mail and any attachments may contain privileged or confidential information. This e-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this e-mail, you are hereby notified that any copying, distribution, dissemination, or action taken in relation to the contents of this e-mail and any of its attachments is strictly prohibited and may be unlawful. If you have received this e-mail in error, please notify the sender immediately and permanently delete the original e-mail and destroy any copies or printouts of this e-mail as well as any attachments.

One attachment • Scanned by Gmail



Fraud via Email



Integrated Systems Corporation
10325 N Port Washington Road
Mequon, WI 53092
(262) 240-7777
www.iscorp.com

May 13, 2022

ISCorp has new banking Information (Since Jan. 2022)

Our Preferred Method is via ACH:

Bank Name: North Shore Bank
15700 W Bluemound Rd
Brookfield, WI 53005

Routing Number: 275071356

Checking Account Number: 27927490

Send all detailed Remittances to: accountsreceivable@iscorp.com

If ACH is not possible, please remit checks to:

ISCorp
PO Box 75278
Chicago IL 60675-5278

Note: Please do not mail checks to ISCorp's HQ address.

We appreciate your cooperation.

Sylvia Diedrich
Sylvia Diedrich
CFO

Sharing

A Look Ahead - Outside

- Cyber
 - No Insurance Coverage without Preventative Measures
 - Single-Sign On (SSO)
 - Multi-Factor Authentication (MFA)
 - Training for Staff - Phishing Campaigns
- Cyber Incident Response Plan
 - [Wisconsin Cyber Response Team](#)

A Look Ahead - Inside

- Positive Pay for AP
- Fraud Hotline or Form?

We operate our own Fraud Hotline. Voicemail access is given to our Internal Audit Manager, Human Resources Director and Finance Director to help avoid the opportunity for one person to cover something up. We also have a e-form on our website where people can submit things and those submissions also get emailed to the same group.

Matthew Hawkesworth
Director of Finance
City of Pasadena
Pasadena CA

Questions?

Fonts & colors used

This presentation has been made using the following fonts:

Archivo Black

(<https://fonts.google.com/specimen/Archivo+Black>)

Actor

(<https://fonts.google.com/specimen/Actor>)



