

# FRAUD AWARENESS

TREASURERS MEETING

MARCH 28, 2024



# WHAT IS FRAUD?

Fraud is the wrongful or criminal **deception** intended to result in financial or personal gain.

It's the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right.



# WHAT DOES FRAUD LOOK LIKE

## Personal

- Unexplained activity in your bank accounts (under \$4.00 is typically confirming the account is active and the large withdrawal will happen soon after)
- Unexplained credit card charges
- Unsolicited debt collectors offering to settle your alleged debt for a fraction of the said debt
- Unsolicited persons notifying you of money supposedly owed to you. They just need some personnel information and your bank or credit card account number to make the deposit. (do not respond with any information)



# WHAT DOES FRAUD LOOK LIKE

## Church

- Unexplained activity in the church's bank accounts (under \$4.00 is typically confirming the account is active and the large withdrawal will happen soon after)
- Unexplained credit card charges
- Fluctuating loose offering i.e., church, sabbath school, missions, etc. (watch for a pattern)
- Money requested doesn't match receipts or missing receipts (multiple times)



# How to avoid being scammed

- Do not open email from people you don't know.
  - Which email address is legitimate?
    - [a. Karen.hanke@floridaconference.com](mailto:Karen.hanke@floridaconference.com)
    - [b. Karen.hanke@floridac0nference.com](mailto:Karen.hanke@floridac0nference.com)
    - [c. Karen.hanke@floridaconference.com](mailto:Karen.hanke@floridaconference.com)
    - [d. Karen.hanke@floridaconferences.com](mailto:Karen.hanke@floridaconferences.com)
    - [e. Karen.hanke@florid@conference.com](mailto:Karen.hanke@florid@conference.com)
- Be careful with links and new website addresses
- Secure your personal information



# How to avoid being scammed

- Do not open email from people you don't know.
  - Which email address is legitimate?
    - a. Karen.hanke@f1oridaconference.com
    - b. Karen.hanke@floridac0nference.com
    - c. Karen.hanke@floridaconference.com**
    - d. Karen.hanke@floridaconferences.com
    - e. Karen.hanke@florid@conference.com
- Be careful with links and new website addresses



# How to avoid being scammed

- Never give your personal information until you independently confirm who and why this information is being requested
- Use strong passwords
- Stay informed on the latest cyber threats
- Be suspicious if someone contacts you unexpectedly online or phone call and asks for your personal information
- It doesn't matter how legitimate the email or caller may look or sound



# How to avoid being scammed

- If it sounds too good to be true, it is. Stop all communication!
- Be cautious if they look questionable, or you get that “bad feeling”
- Get the caller’s name and phone number
- Don’t be afraid to ask the caller to call back later to give you time to confirm who they are
- Independently, contact the vendor and see if they can confirm the caller and the purpose of the call



# How to avoid being scammed

- Only open emails, respond to text messages, voicemails, or callers that are from people or organizations that you KNOW
- Don't let anyone scare you into sending money or providing personal information
- Verify before you trust



# What can fraud in your church look like?

- Employee / Volunteer
- Vendor
- Customer / Member
- Investment scams
- Others



Fraud is a persistent risk that doesn't discriminate by size or type of organization. Fraud is an equal-opportunity problem.



# NAD Working Policy

S 04 48 Dealing with Offenders – When a volunteer or an employee of the Seventh-day Adventist organization performs an **act in violation of the laws of the country and of the financial trust** or responsibility reposed in him / her, **discipline shall be administered, and the organization will report all violation(s) to appropriate law enforcement officials.**



# How to Minimize Fraud

## Prevention and Detection

=

## Internal Controls



# Prevention

- Reconciliations: Have one person prepare the monthly reconciliations
- Limit the number of bank accounts, preferably to just one
- Present original software reports to the board, not just PowerPoint, Excel spreadsheets or any other kind of presentation
- Separate cash related duties: Set up a vendor, approve payments for that vendor, write checks to that vendor



# Prevention

- Improve security on physical (petty cash) and electronic sources of funds
- Utilize 2 or more unrelated people to count the weekly offerings
- Regularly review financial transactions – bank account, credit cards, investments, etc.
- Let unknown callers go to voicemail
- Delete – don't open – unsolicited email
- Verify before you trust



# Detection

- Reconciliations: Have someone other than the preparer review and approve the monthly reconciliations
- Review the financial statements. Watch for variances (budget vs actual and historical comparison)
- Reconcile the weekly offering count sheet with the weekly deposit



# Now what?

What to do if you think fraudulent activity has taken place.

- Contact the vendor, credit card company, bank, pastor / principal, church / school board, etc. and inform them of the fraudulent activity
- Change your passwords
- Collect all the pertinent information and documents regarding the fraudulent activity



# Now what?

- Contact your local police department. Many police departments now have a Fraud Department
- Request the credit bureaus to put a “fraud alert” on your credit file:

Equifax	Experian	Transunion
<p>Fraud alert</p> <ul style="list-style-type: none"><li>• Security freeze</li><li>• 1-800-525-6285</li></ul>	<p>Fraud alert</p> <ul style="list-style-type: none"><li>• Security freeze</li><li>• 1-888-397-3742</li></ul>	<p>Fraud alert</p> <ul style="list-style-type: none"><li>• Security freeze</li><li>• 1-800-916-8800</li></ul>



# Now what?

- Check your insurance coverage for fraud theft insurance
- Consider changing behaviors and building your resistance to fraud
- Don't blame yourself for being victimized.
- Fraudsters are very good, and getting better at what they do. However, you may want to consider the events or actions that may have led up to the fraud.
- As the saying goes, "fool me once shame on you, fool me twice shame on me."



Verify before you trust

