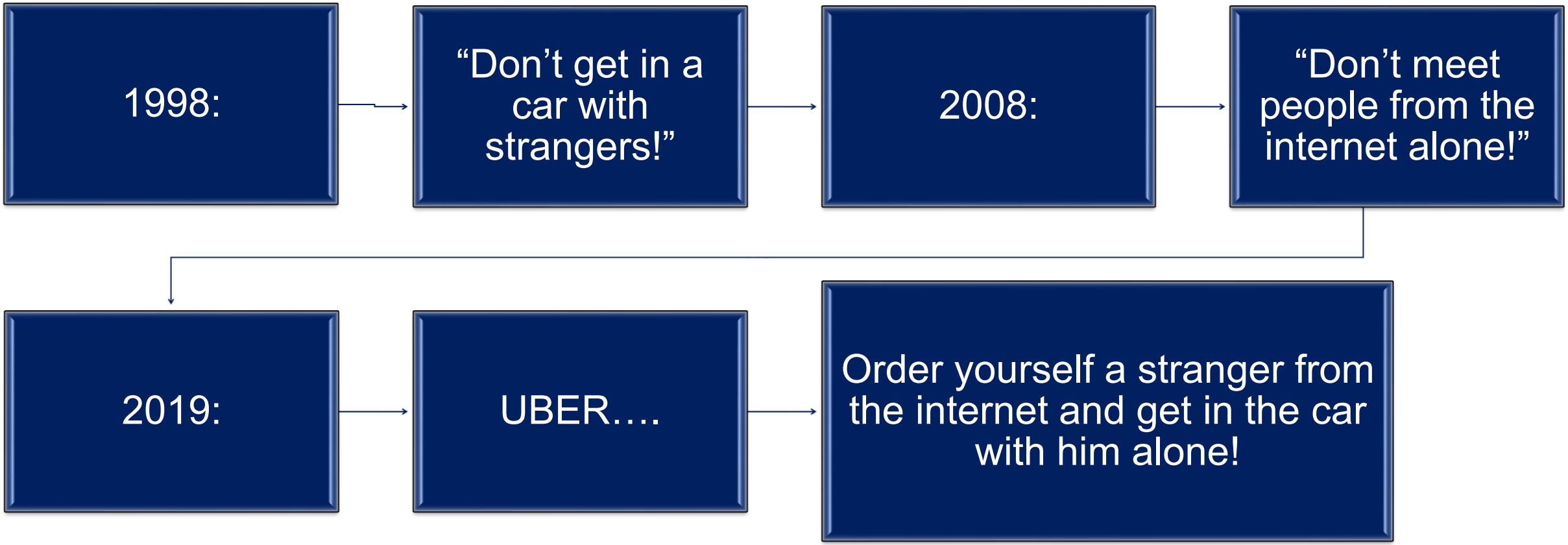
WINTRUST
GOVERNMENT FUNDS

Fraud Scam & Awareness

Ray Olsen CAFS, CAFP, CFS, CBAP
SVP, Senior Director Enterprise Fraud Management

Aimee Briles
SVP, Director of Government Banking
Wintrust Financial Corporation

Times have really changed; we must adapt!



Deep Fakes and Impersonations

- **Deepfakes and AI-powered impersonations** are a growing threat that uses manipulated audio, video, and images to deceive people for financial, political, or social gain. As the technology to create deepfakes becomes more advanced and accessible, the fakes become harder for both humans and traditional detection software to spot.

- **Sophisticated Cyber & External Fraud (2026 Trends)**
- External threats have evolved to use advanced technology to bypass standard verification.

- **AI-Enhanced Phishing**: Scammers use AI to craft near-perfect emails that mimic the tone and style of high-ranking officials (e.g., the Mayor or City Manager) to request urgent wire transfers or sensitive data.

- **Vendor Impersonation**: Criminals monitor public warrant registers (lists of city payments) to identify regular vendors and then send fake requests to change payment or bank account details.

- **Deepfake Media**: In 2025 and 2026, fraudsters have increasingly used deepfake voices or video in "phantom hacker" or imposter scams to trick finance staff into authorizing transactions.

- **ACH & P2P Fraud**: Unauthorized electronic transfers via ACH or peer-to-peer payment apps are growing concerns as municipalities move away from paper checks.

SCAM – RED FLAGS

1. **Scammers PRETEND to be from an organization you know.**

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations. They use technology to change the phone number that appears on your caller ID. The name and number you see on Caller ID might not be real.

2. **Scammers say there's a PROBLEM or a PRIZE.**

They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer. Some scammers say there's a problem with one of your accounts and that you need to verify some information. Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

3. **Scammers PRESSURE you to act immediately.**

Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story. They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted. **"Act Now!"**

4. **Scammers tell you to PAY in a specific way.**

They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back. Some will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money.

Telephone and Texting Scams

Business Email Compromise (BEC) SCAM

(BEC) is a type of phishing or social engineering attack where cybercriminals impersonate legitimate individuals, often executives or business partners, to trick employees into transferring money, revealing sensitive information, or taking other harmful actions.

Subject: Vendor Number R123456789XXXX

[Stop. Think. Read. **This is an external email. Please use caution when clicking on the links and opening attachments in unsolicited email.]**

Dear Support Team,

I am writing in reference to the captioned subject to bring to your attention that we are currently facing challenges as we do not have access to the Self-Service Portal. The individual in possession of the login credentials is presently laid off, prompting the need for urgent action to restore access.

I kindly request your assistance in either resetting the password associated with the portal or **adding me as a new user.** This will ensure seamless access to the platform and enable us to continue our operations without any disruptions.

Could you please guide me on the appropriate steps to take or provide the necessary contacts to address this matter effectively?

Your prompt attention to this request would be greatly appreciated.

Best Regards,
--
Silly Fraudster
Controller/AR
Senior Accounting Technician

Read this email as if you were raised and educated in an English-speaking country, Not the US. UK, Hong Kong, Singapore, India or AI Generated

Behavioral "Red Flags"

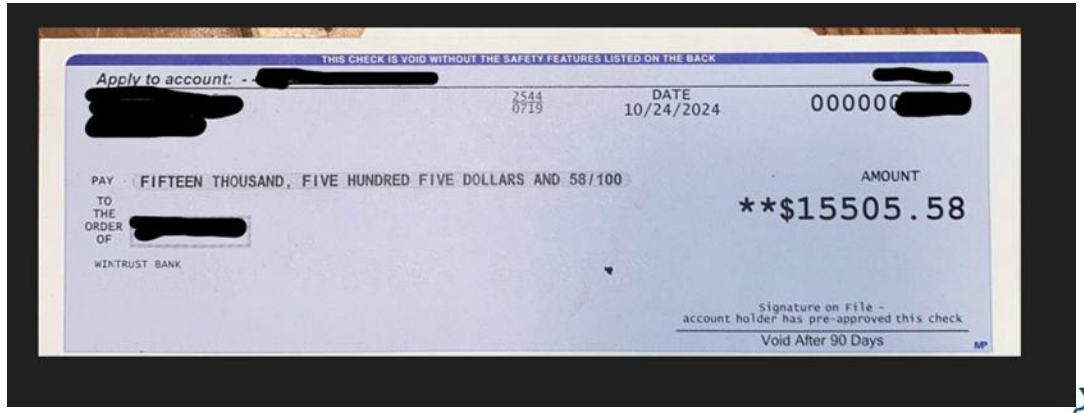
- **Lifestyle Inconsistency**: The most frequent red flag, characterized by sudden, high-end purchases—such as luxury vehicles, designer clothing, or expensive vacations—that do not align with a municipal salary.
- **Compulsive Behaviors**: Signs of addiction, particularly excessive gambling or substance abuse, which often create a desperate need for immediate cash.
- **Refusal to Take Vacation**: Employees may avoid time off because they fear someone else will discover discrepancies in the books while they are away.
- **Territoriality**: Becoming defensive, irritable, or suspicious when colleagues ask standard questions about specific transactions or documentation.
- **Unusual Hours**: Frequently working late, on weekends, or alone in the office when no one is around to witness "last-minute" or manual ledger adjustments.
- **Adjustments Without Documentation**: Frequent month-end adjustments to the ledger that lack supporting receipts or invoices.
- **Lack of Documentation**: Frequent "lost" receipts or missing supporting documents for high-value transactions. In 2026, this remains a high-priority red flag requiring immediate investigation.
- **The "Wheeler-Dealer" Attitude:** An unscrupulous, overly clever, or "risk-taking" approach to business that suggests a willingness to bypass formal controls for perceived efficiency

Fraud Prevention Strategies

- **Out-of-Band Verification:** Bookkeepers, Comptrollers, CPA's, Managers, etc should mandate that any request to change payment instructions or authorize urgent transfers must be confirmed via a pre-established second channel (e.g., a known phone number), never via the link provided in the request.
- **Strengthened Segregation of Duties:** Ensure strict separation between Authorization (approving a vendor), Custody (issuing payment), and Record-keeping (reconciling accounts).
- **Positive Pay**: Implement Positive Pay and ACH Filters with your bank to automatically flag unauthorized transactions before they clear.
- **Independent Audits**: Use outside CPAs or Certified Fraud Examiners (CFEs) for surprise audits and to map internal control systems.
- **Tabletop Exercises**: Conduct regular simulations to test decision-making and response roles for various fraud scenarios, including ransomware and account takeovers. The proverbial "What if".
- **Employee Training**: Train employees to recognize suspicious emails and to verify requests, especially those involving financial transactions. Training cannot be a "One and Done" event!
- **Bank Fraud Calls:** Take your Financial Institution Fraud Department calls seriously. Fraud Analysts make calls for a reason, please listen.

Positive Pay – Best Practices

- Sign up for Check and ACH Positive Pay and Reverse Positive Pay
- Review the exceptions the Bank sent back to you before the cut off time.
  - If you do not know the cut off time, please reach out to your banking professional
- Let your Banker know you identified fraud
- Take your time when reviewing the exception checks…. *They were sent back to you for a reason….*
- Pay Attention to the details and ask yourself this question, ***does the check information match what I uploaded?***
  - Look at the amount
  - Look at the Check Number
  - Look at the Payee
  - Look at the Check Date
  - Has your Company information changed?
  - Are the security features still where they should be?
  - Is the signature correct?



Presenters:

Ray Olsen CAFS, CAFP, CFS, CBAP
SVP, Senior Director Enterprise Fraud Management
rolsen@wintrust.com

Aimee Briles
SVP, Director of Government Banking
Wintrust Financial Corporation
abriles@wintrust.com