

Cash: You've got it, the bad guys want it

How to minimize ACH fraud risks

Puget Sound Finance Officers Association
June 14, 2023

Deborah Pennick, CPA
Assistant Director
Center for Government Innovation



Center for
Government
Innovation



Office of the
Washington
State Auditor

ACH Fraud

How bad is it?

Why should I be concerned?

How does it happen?

How can I minimize my risk?

Where can I find more information?

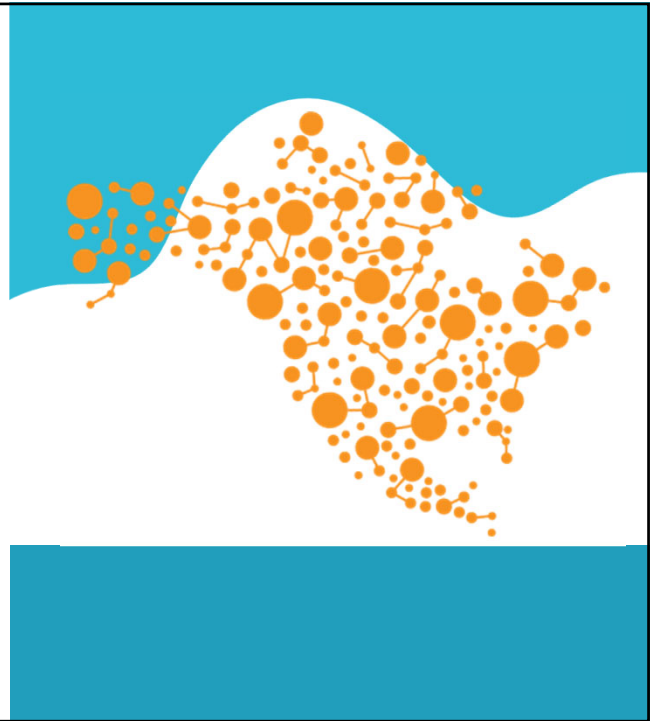


Fun fact:

How many dollars were moved through the ACH Network in 2022?

Answer:

Nearly \$73 trillion



Center for Government Innovation

How bad is it?



Center for Government Innovation

Bad actors are growing in confidence & sophistication



\$2.4 billion

In losses from social engineering, phishing and business email compromise (BEC) attacks

38% increase

In the number of attack attempts from calendar year 2022 to 2021

2nd place

Government/military sustained the most attacks in 2022 after the education/research sector

Center for Government Innovation

Closer to home

Year	Cases	Losses
2022	29	\$4,341,895
2021	13	\$1,944,621
2020	26	\$2,826,064



Center for Government Innovation

Why should I be concerned?



Center for Government Innovation



Any entity type, any size

Center for Government Innovation

Losses can be big



Center for Government Innovation

The chances of recovering funds from a fraudulent ACH are slim to none



Center for Government Innovation

Break the fraud triangle

**Your best defense
is minimizing
opportunity**

Center for Government Innovation



**How does it
happen?**

Center for Government Innovation



Bad actors manipulate our trusting human nature to perpetrate their attacks



Center for Government Innovation



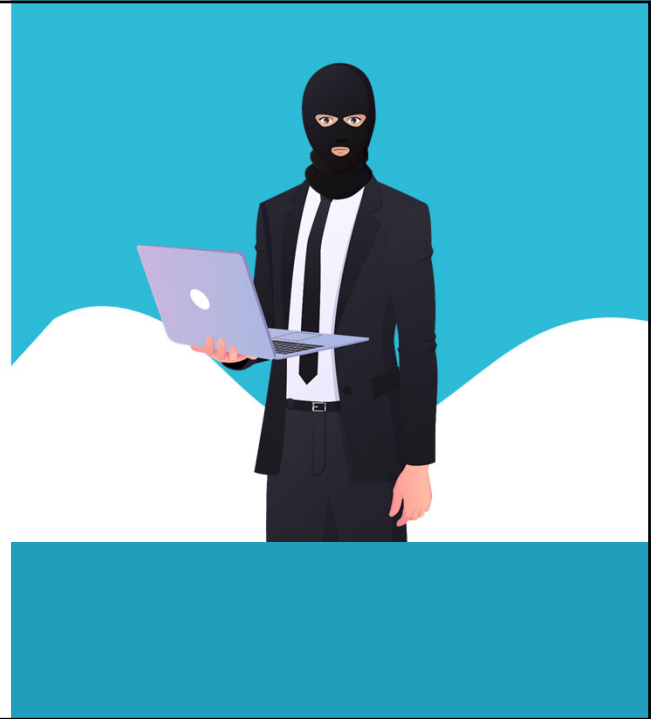
Fraudulent email messages

- **#1 method used by hackers to access your government's data**
- **Designed to trick you into revealing sensitive information**

Center for Government Innovation

Bad actors are clever

- They learn your operations and timetables
- They strategize their plans
- They pose as an employee, vendor or executive management



Center for Government Innovation

How can I minimize my risk?



Center for Government Innovation

Start with a detailed ACH payment policy

- **Process to initiate, approve and execute**
- **Additional segregation of duties**
- **Required safeguards**



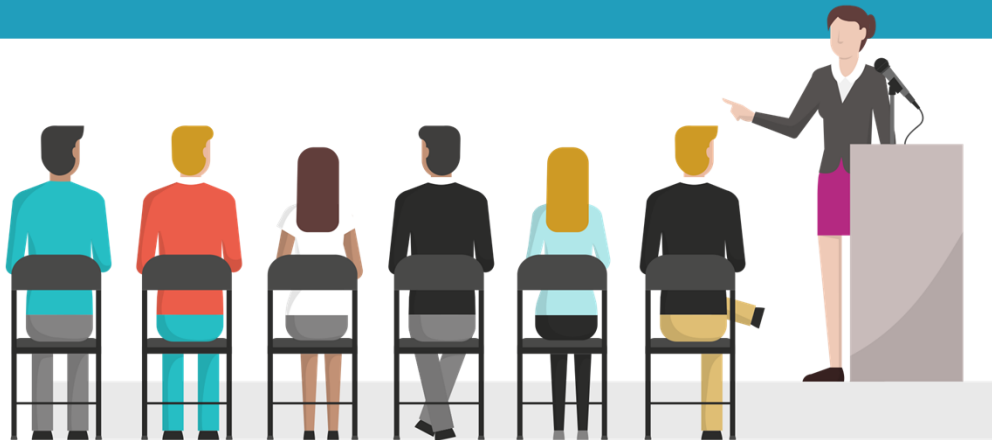
Center for Government Innovation



Center for Government Innovation

Share knowledge of suspicious activity immediately

Educate and train all employees about social engineering and to be responsibly suspicious



Center for Government Innovation



Center for Government Innovation

Minimize your risk

- **Slow down**
- **Consider the source**
- **Question the unusual**
 - **Spelling errors**
 - **Uncommon grammar**
 - **Odd names and titles**



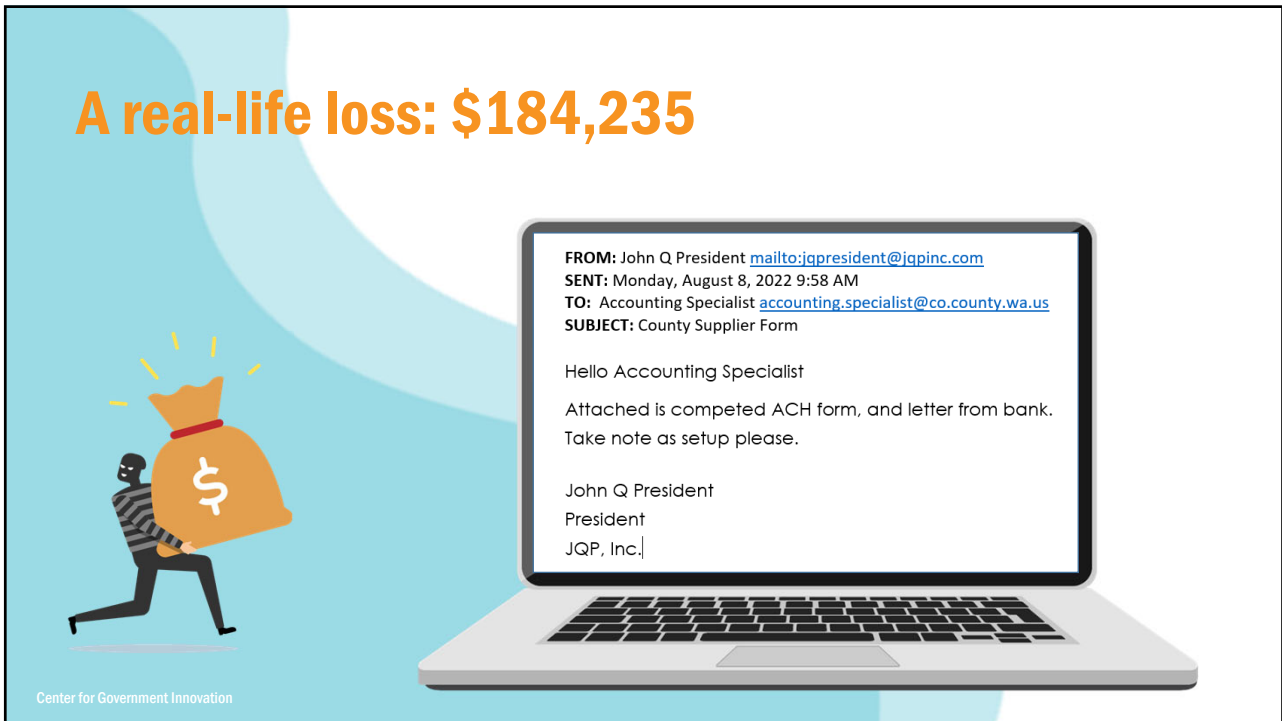
How it happened...

Administrative services forwarded a vendor email requesting bank account changes to Public Works, who then provided the vendor ACH payment form.

A real-life loss: \$184,235

Center for Government Innovation

A real-life loss: \$184,235



FROM: John Q President <mailto:jqpresident@jqpinc.com>
SENT: Monday, August 8, 2022 9:58 AM
TO: Accounting Specialist accounting.specialist@co.county.wa.us
SUBJECT: County Supplier Form

Hello Accounting Specialist

Attached is completed ACH form, and letter from bank.
Take note as setup please.

John Q President
President
JQP, Inc. |

Center for Government Innovation

Minimize your risk

ALWAYS:

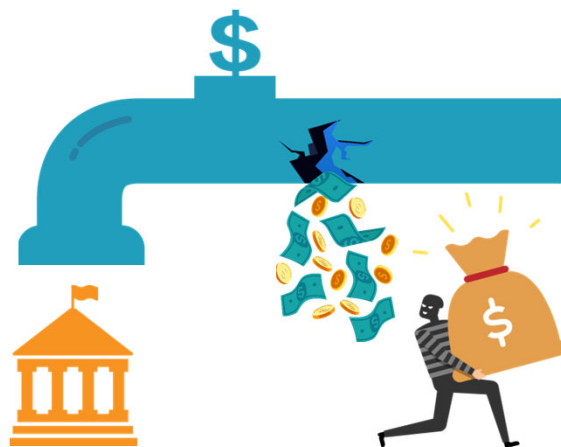
- **Verify requests with known, reliable sources**
- **Provide written notifications of account changes**
- **Use data encryption**



Center for Government Innovation

How it happened...

A Parks Department employee forwarded a vendor email to Accounts Payable requesting an update to banking information. The vendor email had been hacked.



A real-life loss: \$95,444

Center for Government Innovation

Fun fact:

What percentage of Americans get paid using ACH direct deposit?

Answer:

93%

Center for Government Innovation


An illustration on a white background. A large blue pipe with a dollar sign (\$) on top is shown. Money is leaking out of the pipe. On the left, a thief in a black and white striped shirt is running away with a large brown money bag. On the right, there is an orange icon of a classical building with columns and a flag on top, representing a bank.

How it happened...

A bank sent Finance a notification that a payroll direct deposit account had been closed. Finance notified the employee, who had never requested a bank account change.

A real-life loss: \$14,015

Center for Government Innovation



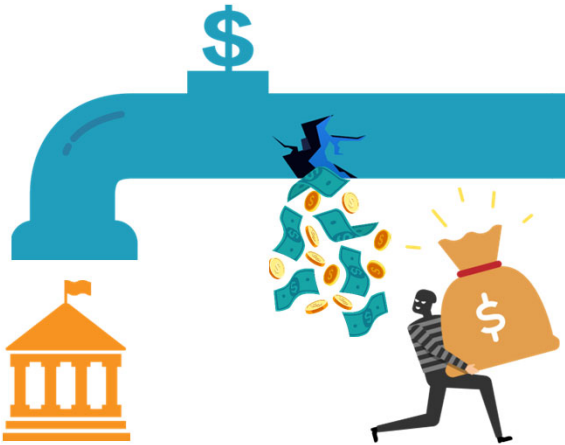
Center for Government Innovation

Minimize your risk

- Use extra precautions with links
- Require complex, unique passwords
- Safeguard passwords

How it happened...

Personal banking information was compromised because employees clicked a phishing email and had their direct deposit information changed.



A real-life loss: \$0

Center for Government Innovation

Minimize your risk

- Detailed policy review
- Urgent requests
- Expressions of anger
- Number/timing of requests

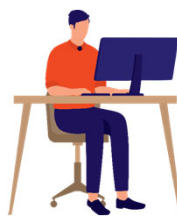


Specialized training for staff who process ACH transactions

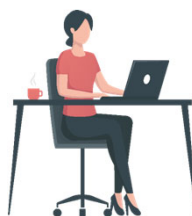
Center for Government Innovation

Minimize your risk: Segregate duties

Segregate Duties



Submit ACH
Payment file



Authorize ACH
Release



Bank Releases
Funds

Center for Government Innovation

Minimize your risk: Segregate duties

Other employees should:

- Review and approve ACH changes and new accounts
- Manage vendor/employee master files
- Monitor/reconcile bank accounts



Center for Government Innovation


An illustration showing a large blue pipe with a dollar sign (\$) on top. The pipe is leaking a stream of money (bills and coins) into a brown bag held by a thief. The thief is wearing a black and white striped shirt and a black mask. Below the pipe is an orange icon of a government building with a flag on top. The background is white with a blue wavy shape at the top.

How it happened...

A Finance Director had full access to all systems as well as ACH/wire transfer capability with little to no oversight or monitoring of her activities.

A real-life loss: \$6,948,277

Center for Government Innovation



Center for Government Innovation


Minimize your risk

- **Dedicate a bank account for ACH transactions**
- **Use ACH positive pay**
- **Consider a bank account validation service**

Minimize your risk

Share ACH information wisely

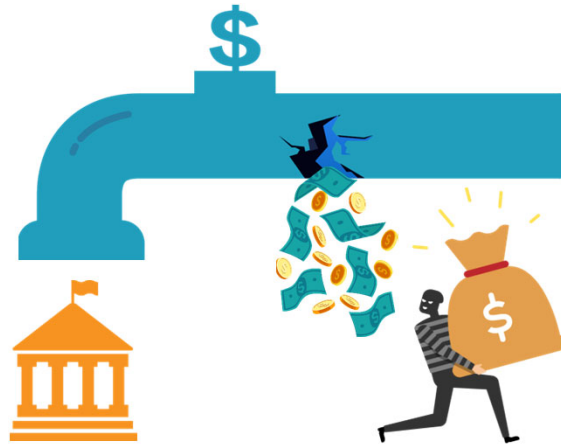
- **Restrict access to ACH forms**
- **Share bank information securely**
- **Safeguard sensitive information**
- **Consider a payee portal**



Center for Government Innovation

How it happens...

A new Payroll Clerk's contact information was added to a City's website. Within days, phishing emails impersonating employees requesting bank account changes started coming in.



Center for Government Innovation

How it happens...

During a Board meeting, the CFO noticed that banking information was listed for ACH transactions on the meeting agenda.



Center for Government Innovation

Minimize your risk

**Make the best of
a bad situation**



Center for Government Innovation

Where can I find more information?



Center for Government Innovation


Resources

Center for Government Innovation
Office of the Washington State Auditor
Pat McCarthy

Best Practices for ACH Electronic Payments

Governments are increasingly using Automated Clearing House (ACH) payments to pay employees and vendors, replacing more costly checks and warrants. These are electronic banks to bank payments processed in batches through the ACH Network. They have their own unique risks that are different from checks and warrants, and these risks are too large to ignore.

Today, bad actors target ACH transactions using social engineering or by having direct system access. In social engineering schemes, bad actors may pose as vendors to get employees to approve changes to contact and/or bank account information in order to divert payments. Employees and others with system access can also perpetrate fraud, such as by adding fictitious vendors or changing a vendor's bank account information to their own or that of an accomplice.




Center for Government Innovation
Office of the Washington State Auditor
Pat McCarthy

Best Practices for ACH Electronic Payments | 4

- Establish dollar limits with your bank. You can establish dollar limits per day or transaction. To determine this limit, you might consider the amount of monthly coverage you have for this purpose.
- Place ACH checks on all other bank accounts. An ACH check presents a higher risk than a check because it is not subject to the same level of scrutiny as a check.
- Consider an ACH three-factor authentication (3FA) solution. 3FA requires the user to provide three different pieces of information to verify their identity. This can be a combination of something you know (password), something you have (a security token), and something you are (biometric data).

Protect the banking information you maintain

- Review access to ACH related items. Do not give an ACH payment system access to anyone who does not need it. Review access to the system and update your access list as needed. Do not give access to the system to anyone who does not need it. Review access to the system and update your access list as needed.
- Share banking information sparingly. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.
- Limit access to sensitive information. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.




Resources

Center for Government Innovation
Office of the Washington State Auditor
Pat McCarthy

Best Practices for Sending Wire Transfers

Wire transfers move money from one bank account to another almost instantaneously. They are generally considered safe as long as the sender is confident the transaction is valid, and the wiring instructions are accurate. In today's environment, those can be hefty assumptions.

Wire transfers are typically used to transfer larger sums of money, and usually only for limited purposes due to the higher transactional cost. For example, governments might use them to make investment purchases, debt payments, or potentially to purchase property.



Center for Government Innovation
Office of the Washington State Auditor
Pat McCarthy

Best Practices for Sending Wire Transfers | 3

Take steps to reduce your risk

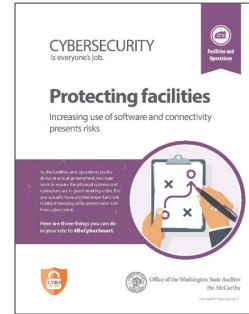
- Prepare your bank's wire transfer system with the bank's internal controls. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.
- Verify the recipient's name and address. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.
- Verify the recipient's account number. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.

Prepare your bank accounts for wire transfers

- Use a dedicated bank account for wire transfers. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.
- Establish dollar limits with your bank. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.
- Place ACH checks on all other bank accounts. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.
- Consider an ACH three-factor authentication (3FA) solution. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it. Do not give your banking information to anyone who does not need it.



Cyber Resources



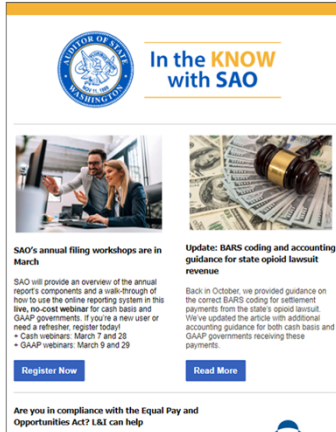
#BeCyberSmart

More Resources



Center for Government Innovation

Subscribe to SAO's e-newsletter



Two ways to sign up:

1. Via SAO's website at sao.wa.gov
2. Use the QR code below:



Center for Government Innovation

Smart governments know cyber health is key. Talk to the Center about a free checkup!

#BeCyberSmart



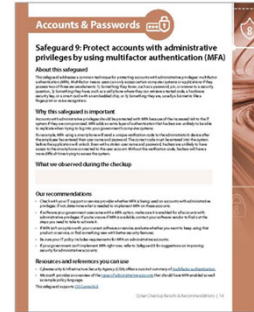
Center for Government Innovation

Why get a Cyber checkup?

Our new checkups offer:

- A fast, free and independent assessment
- Talking points to help guide discussions
- A way to ensure your program is focusing on the right things
- Recommendations to help justify budget requests for tools

Center for Government Innovation



To schedule a checkup for your government, contact the Center:

- Phone: 564-999-0818
- Email: center@sao.wa.gov
- Website: sao.wa.gov

#BeCyberSmart

Center for Government Innovation



Contact information

Debbie Pennick, CPA
Assistant Director
Center for Government Innovation

Deborah.Pennick@sao.wa.gov
center@sao.wa.gov

