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 bank-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.

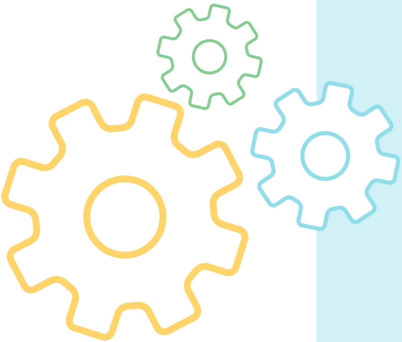
Today, bad actors target ACH transactions using social engineering or by having direct system access. In social engineering schemes, bad actors may pose as vendors to get employees to approve changes to contact and/or bank account information in order to divert payments. Employees and others with system 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.

Governments need to make sure they are sending money to the right place **before** they initiate ACH transactions, as they are final once executed. The National Automated Clearing House Association (NACHA) governs the ACH Network, and its rules accommodate some attempt at recovery. For example, the originating bank can request a return of funds, but the receiving bank does not have to honor the request and they are under no obligation if the money is gone. Most of the time, fraudsters move the money out quickly.

Governments can dispute an unauthorized ACH withdrawal that might appear on their bank statement. However, while a consumer has 60 days to do so, a government has less than two banking days. Each bank will communicate its deadline, as it must initiate a return of the ACH debit by the start of the second business day following the transaction in question.

It is critically important that governments design and implement a robust set of internal controls over ACH payments. To help you, we have compiled these ideas and best practices to help you build stronger ACH controls.

Take these important first steps



- **Develop a detailed ACH payment policy.** Your policy should detail the procedures to initiate, approve and execute ACH payments. It should also describe how employees will verify new or changed payee account information, address segregation of duties, and instruct employees on how they should share information with payees. Your policy should incorporate as many of the best practices below into your procedures, as you deem appropriate.

- **Educate and empower your finance staff to be responsibly suspicious.** Management should provide employee training on social engineering and ACH fraud schemes immediately upon hiring new employees and annually thereafter. Employees need to know that any phone call, email, fax, or letter could be a fraudster and to proceed with caution. For example, employees should be careful about the information they give out over the phone, ask questions of vendors and other employees, and corroborate information with other sources. They also need to know how to spot red flags, such as requests to change banking information just prior to a large payment or a change to both the vendor contact and bank account within a short time period. Your training should also inform employees about your policies and procedures for ACH payments, create a perception of fraud detection within the organization, and share knowledge of consequences for committing fraud.

Assess your financial exposure to ACH fraud

- **Understand NACHA rules and the bank's terms and conditions.** Governments initiating ACH payments have no dispute time period after the ACH transaction is released, but NACHA rules permit some attempt at recovery. There is a short dispute window for ACH debits (unauthorized withdrawals) unexpectedly posted to a government's bank account. Make sure that you understand these rules and the terms of your banking agreement. That way, you can design internal controls appropriately and understand the liability you are assuming when engaging in these transactions.

- **Understand your insurance coverage for ACH losses.** Read your policy, and work with your legal counsel if you need assistance understanding its terms and conditions for ACH payment losses. Obtain additional coverage if you need it, including potentially bonding certain employees.

Segregate duties to reduce your risk

- **Require two different people to execute ACH payments.** Establish a protocol with your bank where one employee submits the ACH payment file and a second employee authorizes release of the funds after verifying the accuracy of the ACH transactions in the batch.

- **Separate processing from editing payee master files.** Employees who process accounts payable or payroll should not have the ability to edit the respective vendor and employee master files.

- **Separate processing from payments.** Employees who process accounts payable or payroll should not create, handle or approve ACH payment files.

- **Keep banking responsibilities separate from the ACH payment processes.** Employees who have authority to add or edit ACH blocks or filters to bank accounts—or have responsibility to monitor or reconcile bank account activity—should not play any part in the ACH payment process.

Prepare your bank accounts for ACH payments

- **Use dedicated bank accounts for ACH transactions.** Maintain a zero balance and restrict these accounts from processing checks or other payment types.

- **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 insurance coverage you have to cover such a loss.

- **Place ACH blocks on all other bank accounts.** An ACH block prevents all ACH activity in any account not used for this purpose.

- **Consider an ACH filter (also known as ACH positive pay).** For bank accounts where you expect to have ACH activity and would like more control, this tool allows you to monitor ACH activity and block incoming charges before they are deducted from your account. This tool will also send notifications of any activity outside of the parameters that you establish for payees (e.g., name, dollar limits, timeframe).

Protect the banking information you maintain

- **Restrict access to ACH-related forms.** Do not place ACH payment sign-up forms and forms to update payee account information on your public-facing website. This limits access and makes it more difficult for bad actors to make fraudulent requests appear legitimate.

- **Share banking information securely.** Payees should use encryption when emailing bank information to you, to reduce the risk of alteration during transit. Even with encryption, your staff should still verify the new information directly with the payee.

- **Limit access to sensitive information.** Securely store and protect payee banking information. Only one or two employees should have the ability to edit employee or vendor banking information. Additionally, permissions to view this sensitive information should be limited to those who need it to do their job.

- **Secure your vendor or employee self-service payee portal.** A payee portal can be a better option than relying on emails as long as it is secure and you actively manage user access. A payee portal should have strong security measures, such as automatic log-off after inactivity, strong password requirements, and multifactor authentication for verifying identity. Additionally, ensure that you install all software updates and patches promptly. The Government Finance Officers Association (GFOA) also advises portals have approvals or notifications related to changes, as well as audit trails.

- **Electronic payment files should be secure and read-only.** You should securely prepare, store and transmit ACH payment files to protect the information they contain. The payment file should be read-only. If anyone can edit the payment file, your fraud risk increases significantly. You would then have to monitor the payment file for any unauthorized changes, from creation of the file up to bank submission.

Set up a payee verification process

- **Assign a passcode or passphrase to payees.** Payees can provide this information as additional proof of their identity when speaking with your staff. You should also teach your vendors and employees how to protect passcodes or passphrases. For example, they should not be stored online, emailed (unless encrypted), or shared with other employees.

- **Verify accuracy of payee information.** It is critical that staff verify new payee account information and any subsequent changes by phone (a video call could work if staff would recognize the payee). Your staff should verify changes to contact information (name, phone, and email), mailing addresses or banking information, regardless of how they are provided (including within a self-service portal). Your staff should use known and reliable contact information that is already on file and has been previously used. They should not use contact information from recently provided information, such as an email. If possible, employees should make changes in person.

- **Consider implementing account validation.** You can choose to validate the accuracy of account information, and possibly account ownership, using different methods. These methods include an ACH pre-notification, ACH micro-transaction verification, or a commercially available validation service (such as those offered by some banks). It is up to you to determine frequency, such as at enrollment or before sending each payment. To learn more about account validation, see the NACHA resource on this topic.

Changing contact information can be a first step in a fraudster's scheme to eventually change bank account information.

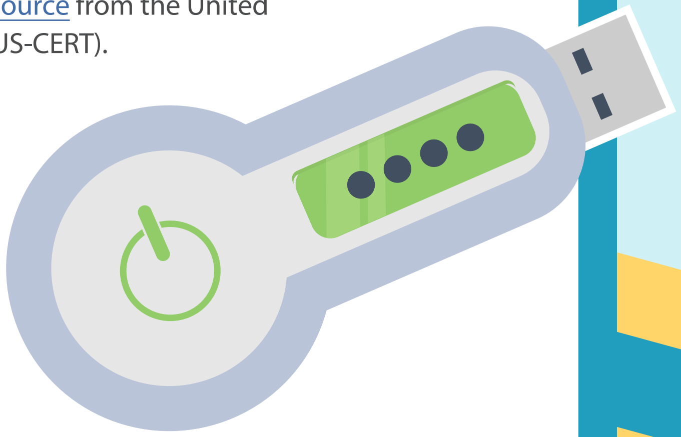
- **Review verification documentation.** Management should review and approve verification documentation before staff enter changes into the system.

- **Review all payee account changes.** Management should review all payee account changes that occur up to creation of the ACH payment file (or up to submission to the bank if the ACH payment file can be edited). One way is to compare a system exception report that details all changes since the last payment run to the source documentation.

Take steps to protect yourself when using online banking

- **Use a dedicated, secure computer.** You should send ACH payment batches using a computer solely dedicated to online banking activity. This computer needs to be up to date with security patches and antivirus protection. These measures protect it from malware, which can lead to compromised login credentials. You can learn more about how to bank securely online by reading this resource from the United States Computer Emergency Readiness Team (US-CERT).

- **Use a bank that offers token keys.** A token is a physical device that provides a key code you enter when logging into your online account. This form of multifactor authentication is more secure than an emailed or texted code. Governments should contract with banks that offer this security device and use it for any employee that has entitlements to send or release ACH payment batches.



- **Keep up to date on your bank's security measures.** Check in with your bank every six months to identify new options or services that can help protect your government against ACH fraud.

Actively monitor

- **Check the bank's ACH remittance receipt.** Immediately after you have initiated your ACH transaction, compare the bank's ACH receipt to your original documentation.

- **Review your bank account daily.** To identify issues promptly, governments engaging in ACH activity should review bank accounts and ACH activity at least daily.

- **Periodically review payee lists.** You should periodically review your employee and vendor master files for red flags like duplicate records or vendors and employees with matching bank accounts (an indicator an employee may be fraudulently diverting vendor payments to a personal account).

- **Follow up on vendor complaints promptly.** You should act promptly if any vendor reports it has not been paid. It is possible that the payment was fraudulently diverted, and acting promptly can aid in the recovery efforts.

- **Use fraudulent incidents to inform your risk assessment process.** Analyze and quantify the extent to which your government has already suffered financial losses from fraudulent ACH payments to inform fraud risk assessments and prioritize and tailor countermeasures.

Additional resources

- National Automated Clearing House Association's (NACHA)
  Account Validation: A tool for businesses to improve ACH Transactions

- National Automated Clearing House Association's (NACHA)
  Protecting against cyber-fraud

- United States Computer Emergency Readiness Team's (US-CERT)
  Banking Securely Online (cisa.gov)

- Government Finance Officers Association's (GFOA)
  Advisory on Electronic Vendor Fraud

- Office of the Washington State Auditor's
  Segregation of Duties guide

For assistance

This resource was developed by the Center for Government Innovation at the Office of the Washington State Auditor. Please send questions, comments, or suggestions to Center@sao.wa.gov.

Disclaimer

This resource is provided for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation, or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.

Center for Government
Innovation