citi

Chief Information Security Office

Manual and Electronic Payment Security Best Practices

The rise in digital banking has created more efficient and accessible ways to move money, but e-payment systems have also created new tools for fraudsters to exploit.

Manual payments

What are the risks?

Traditional manual payments can be counterfeit, particularly with modern desktop applications that allow anyone with a computer to forge cheques, company letterheads, etc.

- **Signatures are also easily forged**. Authorized company signatories can easily be obtained by intercepting cheques or company documentation in the post.
- **Multiple vulnerability points exist in the manual payment process that make them easy to intercept**. Paper transactions can be intercepted enroute to the bank or from the mail or point of sale, where they can be stolen or where beneficiary details can be captured and subsequently altered to redirect funds to fraudulent third-party accounts.
- **Delays in account reconciliation increase the late detection of fraud, to include internal fraud**. A manual paper transaction request could be entirely fabricated by an internal source and placed in a batch of daily paper transaction requests to redirect funds to an external fraudulent account.
- **Manual payments can often be initiated without adhering to control processes**. The manual nature and volume of payment request can lead to workarounds such as pre-signed cheques and documents that create more unnecessary fraud risk

How do you protect against this type of fraud?

If it is necessary to make manual payments, there are several measures that you can take:

- For payments you make regularly, establish standard settlement instructions that are properly authenticated. Once this is set up, all payments should only be made to the designated account.
- Segregation of Duties (SoD): Enforce a multi-level approval workflow so that the person initiating a payment is different from the person approving and releasing it. This prevents a single individual from controlling the entire process.
- Implement strict approval procedures. Do not accept amendments or any irregularities, such as changes in bank details, irregular amounts, or payments to unusual location without proper authentication, including verification of account number and beneficiary bank. For example, a request to amend a payee's bank account details should be verified by a recorded callback process using a properly authenticated and independently sourced number with a designated supplier contact.
- Manual transfer requests should be executed with additional levels of approval. Require a second or even third person to verify the details of any significant payment before it is made. This is especially important for larger payments.
- Establish clear, written policies and procedures for all manual payments. Ensure all staff are trained on these procedures, including the prohibition of non-approved communication channels (e.g., personal email, messaging apps, etc.) for communication and handling payment instructions.

- Pre-established, verifiable forms that do not deviate from prior transmissions should always be used.

Electronic payments

Why are they more secure?

Electronic payments offer some compelling advantages:

- They are encrypted and can be protected with Multi-Factor Authentication (MFA) and with multilevel authorizations and approvals.
- They are swift compared to manual transfers and to carry significantly reduced risk of being intercepted; funds transfer requests are securely encrypted.
- Electronic signatures are cryptographically secured against unauthorized forging. Entitlements and authorizations can be further supported by secure Multi-Factor Authentication (MFA) and multilevel approvals.
- Frequent reconciliation allows accounts to be proofed or reconciled in near real-time allowing for the detection of anomalies promptly, potentially preventing additional fraudulent activity.
- Internal processes can be enforced systematically. Entitlement and authorization limits can be set in accordance with risk.
- They allow for remote access. Transactions can be carried out without the need for high-risk contingency or exception processes if key personnel are out of the office.

Are there any risks?

Despite their greater security, electronic payments aren't without risk. Employees may be deceived into making or authorizing payments to fraudulent accounts via social engineering (e.g., impersonation including deepfake voice/video, urgent executive requests). Either intentionally or unintentionally, passwords can be compromised. This can happen if passwords are shared or recorded in unsecure locations. There is also the risk of collusion, which involves two parties or employees working together to compromise payment integrity.

Here are some best practices to mitigate e-payment risks:

- Implement strong multi-factor authentication (MFA), which can include biometric methods. Ensure MFA tokens (e.g., authenticator applications, safe word cards etc.) and their associated credentials (like pins) are always kept separate.
- Use strong, unique, complex passwords for all your financial accounts. Do not allow passwords to be shared or compromised.
- Avoid using public Wi-Fi and use a secure, corporate network for any financial transactions to prevent man-in-the-middle attacks.
- Utilize platforms with advanced fraud prevention technologies that analyze device, location, and user behavior in real-time, automatically blocking suspicious transactions before they are initiated to proactively stop fraud. Entitle employees only with appropriate authorization levels.
- Enforce a multi-level approval workflow to have all transactions approved at least by dual control, e.g. impose maker-checker functionality with clearly defined approval limits and authority matrices, including periodic review of senior and privileged user access.
- Impose a timely proofing or reconciliation of accounts so that anomalies can be quickly identified.
- Establish a dedicated suspicious activity management program to continuously monitor for unusual behavior across all internet-facing applications and any payment systems classified as having high or very high criticality.
- Implement and maintain regular, comprehensive security awareness training programs for all employees. This training should cover topics such as identifying phishing attempts, recognizing social engineering tactics (including impersonation and deepfake voice/video), understanding password hygiene (e.g., using strong, unique passwords, and password managers, awareness of authorized payment fraud risks, and adhering to secure payment processing procedures.