# Manual and Electronic Payment Security Best Practice

Banking today is more digitised than ever. Despite the ever-increasing move towards e-payments and the more efficient means of managing payments to suppliers that they offer, sometimes it's still necessary to manually transfer funds. Below we look at some of the risks associated with both payment methods along with some best practices to protect against them.

## Manual payments

### What are the risks?

Manually initiated payments are generally considered to carry more risks than electronic transfers. These carry an inherent fraud risk because of the manual intervention required to complete the transaction. Manual payments include the following associated risks.

- They're easy to counterfeit, particularly with modern desktop applications that allow anyone with a computer to print cheques, company letterheads and so on.
- Signatures are easily forged. Authorised company signatories can easily be obtained by intercepting cheques or company documentation in the post.
- They're easy to intercept. Multiple vulnerability points make them easy to amend. Paper transactions can be intercepted en route to the bank 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 any fraud and the risk of 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.
- They cannot generally be completed remotely, which leads to workaround exception solutions such as pre-signed cheques and documents that create more unnecessary risk.

### How do you fight them?

If it is necessary to make manual payments, there are a number of measures that you can take right now to protect against fraud.

- If you regularly make payments to a particular supplier, you set up a standard settlement instruction that is properly authenticated. Once this is set up, all payments should only be made to that account.
- Do not accept amendments without proper authentication. For example, a request to amend a supplier's bank account details should be verified by a 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.
- Pre-established, verifiable forms that do not deviate from prior transmissions should always be used.

## Electronic payments

### Why are they secure?

Electronic payments are considered to be more secure for a number of reasons, including:

- They are secure and encrypted and can be protected with a secure one-time password (OTP) and with multilevel authorisations and approvals.
- They are swift to deliver and have no risk of being intercepted: funds transfer requests are securely encrypted.
- Signatures cannot be forged. Entitlements and authorisations are supported by secure OTP and multilevel approvals.
- There is immediate and automated reconciliation. Accounts can be proofed or reconciled in real-time allowing for the detection of anomalies in a timely fashion.
- Internal processes can be enforced systematically. Entitlement and authorisation 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?

In spite of their greater security, electronic payments aren't without risk. Either intentionally or unintentionally, passwords can be compromised, for instance. 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. So some best practices to mitigate e-payment risks include the following.

- Ensure safeword cards and pins are always kept separate.
- Do not allow passwords to be shared or compromised.
- Entitle employees only with appropriate authorisation levels.
- Have all transactions approved at least by dual control, e.g. impose maker-checker functionality.
- Impose a timely proofing or reconciliation of accounts so that anomalies can be quickly identified.
- Ensure that high-value transactions always require multiple approvers.

**Treasury and Trade Solutions**
**transactionservices.citi.com**



GRA29064 01/2018