Cash Management: Cash in Transit, Teller Implant and Mobile Teller Services

Cash-intensive businesses and economies are susceptible to fraud and theft from organised criminal groups that perceive corporates as easy targets because their control environments are easy to circumvent. Such groups have been increasingly successful in their attempts to defraud.

Our experience suggests that criminals will take advantage of any opportunity provided by a lax control environment, gaps in existing processes or controls, or altogether absent controls. Knowledge of a process or control or collusive behaviour may also facilitate fraud or theft.

Organised criminals continue to develop more sophisticated and innovative methods to defraud our institution and our clients. In response, our controls are frequently assessed and enhanced to protect you, our clients.

One of the more prevalent types of industry fraud affecting our cash-intensive region is the theft of cash through the impersonation of security cash-in-transit personnel. Below we have listed some of the best practices and preventive measures for cash management and cash-in-transit services including red flags to detect or prevent this fraud type from having an impact on your business.

Here are some best practices

Ensure that the service level agreement with service providers including Citi covers operational processes and that staff are fully aware of their roles and responsibilities. Management should:

- Ensure all employees receive periodic training.
- Ensure access to your premises and teller environment is controlled and restricted at all times.
- Store teller and till stamps, receipt books and forms securely.
- Ensure there is no cash left on the premises at the close of business. If cash is stored overnight in a vault, both the reconciliation and the sealing of cash bags should be performed in the joint presence of the appointed financial controller and the implant teller.
- Confirm the identities of the cash-in-transit personnel against the approved list of photo IDs and signatures provided. Any doubt about identity must be escalated to nominated Citi contacts before any transactions occur with such personnel.
- Ensure dual custody is observed when packing cash for transportation to the cash centre.
- Ensure that the seals on cash boxes and sealed bags are used in sequence prior to transportation and that the same seal numbers are recorded in the shipment manifest and courier receipt(s).
- If practicable, ensure all cash-counting and -handling processes take place in an area or in areas covered by a functioning CCTV camera. This is important from a deterrence and an investigation perspective.
- Ensure all cash received is counted under UV light, using a counting machine where applicable, before handing deposits to the bank.

- Ensure any requests to deviate from the usual or standard procedure are treated as a red flag and confirmed with nominated Citi contacts.*

Here are some preventative controls and principles

- Know your employee starts with pre-employment screening and continues throughout the staff's career. It should not be limited to any level of seniority, e.g. junior employees or employees in responsible positions.
- Know your customer or supplier. For example, only make payments to a previously authenticated beneficiary account. Do not accept any amendments to beneficiary details without proper authentication.
- Understand the risks. Evaluate processes to identify fraud risks and ensure there are mitigating controls in place.
- Ensure staff are trained on business processes and controls and on fraud awareness and controls to prevent and detect fraud and theft.
- Segregation of duties (maker/checker) ensures no single individual has the authority to input (make) and authorise (check) a transaction.
- Dual custody must be in place, for example, custodians to cash vaults and safes.
- Audit trails: systems should be designed to enable individual transactions and account enquiries to be traceable to a specific system user.
- Password sharing: under no circumstances should passwords be shared.
- Timely account reconciliation ensures the prompt identification of anomalies.
- System rights and entitlement management ensures appropriate authorisation levels are reviewed on a regular basis and are granted to employees to perform only the required functions in their job profiles.

Here are some things that constitute red flags*

- Official communication on agent lists from Citi received through any means other than secure Citi email or any other agreed form of communication.
- Collection agents coming at non-scheduled times for cash pickups.
- Collection agents not included on Citi-approved lists.
- Cash boxes or sealed bags supplied or collected with non-sequential, broken or modified seals.
- Collection agents in a rush or under pressure to collect cash delivery.
- Employee lifestyle or behavioural changes, e.g. expensive items beyond salary entitlements like cars, jewellery and homes.
- Significant personal financial debt.
- High employee turnover, especially in areas more vulnerable to fraud.
- A refusal or reluctance of staff to take vacation or sick leave.
- The domination of a particular product or process by a sole employee, i.e. a lack of segregation of duties.

*Red flags are indicators, characteristics or patterns contained within a request (transaction and/or change request for the purposes of cash management) that should be perceived as a warning and may suggest that something is not quite right. On their own, or in combination with additional "red flags", they may constitute suspicious activity and warrant further investigation, prior to any execution.

Nothing herein contained replaces or amends the existing terms and conditions of business as agreed between Citi and its clients, which remain in full force and effect.

GRA25375 08/14