

ESTA Guidance to customers for the selection of cash service providers

Cash services are unique given the value and ease of exchange of the product they deal with. ESTA, the body representing cash management companies in Europe, is pleased to provide the following guidance to potential users of cash services when considering the suitability of a supplier.

The first thing to consider is the type of cash service involved. For these purposes we distinguish between two distinct types of service:

1. **Cash-in-Transit (CIT)** including ATM / device replenishment with or without secured engineering, emptying of ATMs and recirculation of cash; and
2. **Cash Processing** services including customer deposit processing and the provision of cash for ATMs and other recycling equipment.

A. Introduction

1. CIT Services

CIT is the secure transportation of cash that has been placed by the customer in sealed tamper-evident containers/bags/envelopes of various types for transport between two locations. When solely providing CIT, the cash management company staff should never come into direct physical contact with the customer's cash. There may be an exception to this principle when servicing ATMs or other automated cash devices. In some cases rather than exchanging closed cassettes the accepted process is to top up the device with additional banknotes. Similarly depositing devices may require the removal of loose banknotes and coin. In these cases the cash is exposed to the CIT crew.

Security licensed CIT companies are specialists in managing the risk associated with the logistics of cash and ESTA would recommend their use even where fairly modest sums are involved. While the risk to an individual user occasionally using insecure transport for modest sums may appear low, he may not be aware that, if others do the same, the risk pattern may change considerably if criminals realise that cash is being transported unsecured.

2. Cash Processing

Cash Processing involves the opening of sealed, tamper evident cash containers/bags/envelopes, and subjecting the cash to some or all of the following: authentication, validation, counting, sorting, secure storage or onward transfer; reporting or crediting.

As can be seen, Customers should be wary to avoid service providers where direct cash exposure to the supplier's staff and equipment might increase the risk of loss or error in any of the processes involved. In most cases the scale of cash processing operations will mean that substantially more "open" cash will be involved compared to undertaking ATM replenishment services.

3. Risks & Guidance

ESTA believes that from a customer perspective CIT and Cash Processing have fundamentally different potential risks patterns and it is important to understand this when evaluating suppliers.

In this guidance, ESTA first identifies common features that should apply to both CIT and Cash Processing Suppliers and, based on these, recommend specific good practice for CIT or Cash Processing.

This guidance should apply for large scale operations such as those of banks or national retail chains. While many of these recommendations are relevant in most situations, Customers should consider their appropriateness for smaller volumes and values.

B. Common requirements for both CIT and Cash Processing suppliers

- **Regulatory Compliance**

In some European markets CIT and / or Cash Processing is regulated by State bodies and the Customer should explore this for the relevant market.

A Supplier which is authorised to undertake CIT is not automatically authorised to undertake Cash Processing and vice versa. Customers should ascertain that a potential Supplier is approved by the relevant regulatory body for the relevant service. Where no regulatory body exists Customers should take steps to assess the suitability of a Supplier for either type of service, irrespective of whether it is authorised to do the other. This guidance is intended to assist in this process.

Where an association for CIT/Cash Processing companies exists, Customers should preferably choose a supplier who is a member of this association.

- **Insurance**

The Supplier should be able to provide evidence for comprehensive insurance cover for the cash under his responsibility. The Customer should be aware that insurance policies may have exclusions or limitations in relation to fraud by a Director of the company who acts in a proprietorial role. Customers should look at this issue in relation to the services to be provided and ensure relevant measures are taken to mitigate any risk.

- **Financial Resilience**

As for any businesses, Customers should enquire on the financial reliability of the Supplier and estimate the likelihood of the Supplier's business failing during the contract term. The amount of cash to be dealt with by the supplier should be commensurate to the potential risk of business failure.

- **Risk Management**

The Customer should check that in their chosen supplier's company, an Executive is responsible for the management of risk. This person should be independent from those responsible for operating the business. There should be a defined process for assessing and managing risk, the basis (if not the details) of which should be shared with Customers upon request.

- **Vetting**

The Supplier should have a defined vetting process for staff the principle of which should be made available to Customers. All staff should be subject to this process.

- **Business Continuity**

Reputable suppliers should have a business continuity plan in place which addresses risk and mitigation measures for both common and uncommon disturbances.

- **Operating Procedures**

The Supplier should have robust, documented and auditable operating procedures in place.

C. The special requirements of the supply of CIT services

- **Geographic Scope**

The Supplier must be able to provide the CIT service, either directly or through licensed subcontractors (where it applies), within the relevant geographical zone and within the required timeframe for both collection and delivery. This does not just mean collection / delivery to or from Customers but should also include the time taken from collection to delivery at the appropriate cash centre (and vice versa), as this can impact upon the date of account crediting.

- **Value Limits**

The value of cash to be transported will determine in the security systems deployed by the Supplier covering all aspects of the service. Reputable Suppliers will have a range of security system options to deploy and value limits will vary based on the effectiveness of each solution for each specific level of risk. Such a structured approach to risk management should be considered as a criteria for Supplier quality rather than a sign of lack of flexibility.

- **Constraints**

Reputable Suppliers will undertake a risk assessment of their Customer's environment prior to offering/commencing the service. This risk assessment should consider the security system to be deployed. It will identify the constraints under which the selected security system can operate within an acceptable level of risk.

Customers should consider carefully whether such constraints are acceptable before providing any service as they will be central to both the safety of the Supplier and Customer's staff but also to any issues of liability for loss between the two parties.

- **Liability**

The Customer should precisely establish at what point in the service liability for loss passes from the Customer to the Supplier or vice versa and decide whether this is acceptable.

- **Traceability**

Reputable Suppliers will have a full audit trail for any cash containers in their possession and be able to demonstrate to Customers the status of individual items. Many Suppliers will be able to offer the Customer a web portal-based tracking system using information input from CIT crews via handheld terminals and/or intelligent containers.

- **Capacity and Service Recovery**

In a real world, environment service failures, whether arising from the Supplier or the Customer, can happen and disrupt plans. Customers should assess the Supplier's ability to overcome such situations in a way which minimises the consequences to Customers and allow for swift completion of the service.

- **Time Windows**

Many Customers will have specific time-of-day requirements within which the service needs to take place. Although predictable time windows should be avoided for security reasons, the Supplier must be able to operate within these constraints.

- **Staff Quality**

The quality of CIT services depends essentially on the quality of staff and their training. The Supplier should be able to demonstrate a comprehensive approach to recruiting, training and developing CIT staff. Staff should wear uniforms and personal protective equipment at all times.

Compliance to procedures is a key performance criteria in a risk environment, and the service should be delivered with courtesy and professionalism at all times.

- **Performance**

Reputable suppliers will be willing to agree clear and defined service and performance indicators.

- **Terms and Conditions**

Reputable suppliers have a clear and transparent set of terms and conditions in place that form part of any contract between the supplier and the customer.

D. The special requirements of the supply of cash processing services

- **Premises access control**

The Supplier must have systems in place to ensure that access to the premises is secure and controlled. Once in the premises there should be dedicated secure areas within which cash is handled that should be distinctly separate from non-secure areas such as canteens, offices etc. Access to these secure areas should be restricted to the necessary personnel and entry and exit from secure areas should be securely controlled adopting a dual control principle (see below). Tracing records of entry and exit should be maintained.

- **Dual Control**

This is sometimes referred to as "the 4 eyes principle". Throughout the secure areas the Supplier's personnel activity should follow a dual control principle i.e. no one individual in isolation should be able to effect critical actions without a second person being involved. This may be done remotely and the monitoring by CCTV. For example no one person acting in isolation should be able to have access into or out of the secure areas.

- **CCTV**

CCTV coverage should be comprehensive in the secure areas and the video files stored for a defined period. In the event of a dispute between the Customer and Supplier, the latter should be able to produce video evidence of the deposit being processed and with sufficient resolution. CCTV coverage in the non-secure areas and building perimeter should be adequate for the purposes of threat monitoring.

- **Audit Trail**

There should be an audit trail of the movement of Customers' cash through the processing centre from receipt from the CIT vehicle. Ideally this audit trail should be automated. The audit trail needs to be archived for a period long enough to enable effective dispute resolution between any Customer and the Supplier.

- **Cash Storage**

Where banknotes are stored on site overnight, they should be stored in a defined secure area. Where substantial funds are held they should be secured in a vault or strong-room with a rating relevant to the value of funds stored. Camera coverage must continue within the area/vault. While these principles apply to coins, the nature of the storage area should reflect the value stored and the risk of loss given the heavy weight of large values in coin.

The Supplier should regularly provide Customers with a reconciliation of the Customer's funds according to a frequency contractually agreed, showing the value received, the value despatched and the value retained. This should be broken down denominationally and the Supplier should warrant that this is the actual balance stored on the Customer's behalf. If this is not the case any difference should be flagged to the Customer immediately by the Supplier.

There should be an agreed process with defined timescales for the resolution of any such differences. In addition the Customer and the Supplier should agree from the outset a process and timescale by which the Customer can positively confirm agreement of the submitted Supplier-reconciled values with the Supplier. Such a process is important for both parties so that any errors on either side can be identified, investigated and resolved in a timely and efficient manner.

- **Vault Management Systems**

Larger cash centres should be equipped with software-based vault management systems that collect data on all of the internal transactions within the cash centre and provide reconciliations, reports and electronic data files.

- **Right of Access and Audit**

Where substantial cash balances are stored overnight, the Customer should have a defined right of access and right to unannounced audit. Such access will need to be arranged so as not to undermine either the security of the site or the customer's ability to undertake effective unannounced audits for the purpose of verification of cash balance.

- **Equipment**

All equipment used on site for authentication and recirculation of cash should be subject to a maintenance schedule and the customer should have the right to inspect this schedule during an audit. Where banknote fitness sorting is undertaken for recirculation of banknotes via automated devices then any relevant Central Bank regulations or guidelines on the selection, operation, calibration and maintenance of such equipment must be complied with and the Customer should have the right to audit appropriate records.

- **Power and Systems Loss**

In relation to the risk inherent to the site and the impact upon the Customer's business, the Supplier will have appropriate back-up and systems redundancy in place to deal with losses of power or IT failure. At the very least the site will in the event of a power failure have back-up supplies to ensure that relevant CCTV and alarm systems are sustained for sufficient time to assure security.

- **Dispute and Claims Resolution**

There should be mutually agreed and documented disputes & claims process with defined accountabilities, timescales and outcomes.

- **Service Levels**

There should be mutually agreed and documented service levels with defined methods of measurement and reporting.

- **Procedures and Training**

The Supplier should be able to provide evidence to the Customer that appropriate documented procedures exist for all the tasks within the cash centre and any security situation or external event that may be reasonably anticipated. The actual contents of these procedures may remain confidential to the Supplier. The Supplier should be able to provide evidence that relevant staff have been trained in these procedures and with the relevant equipment. During audits the Customer should be allowed to verify that staff undertaking tasks has received adequate training with relevant records.

- **Framework Compliance**

The local central bank may have guidelines and/or a framework in place that details the National rules for the cash cycle. A reputable supplier will be aware of these requirements and be able to demonstrate compliance. Similarly the Supplier should be aware of any applicable laws related to the authentication and recirculation of cash and be able to demonstrate compliance.