ATM Service Providers (CIT Carriers) Best Practices Guide

International minimum security guidelines and best practices ATM service providers

Developed by:

Cash Connect
115 College Square
Second Floor
Newark, DE 19711
302-283-4100
www.cash-connect.com

Endorsed by:

PO Box 88433
Sioux Falls, SD 57109-8433
www.atmia.com

In Association with:

American Special Risk, LLC
212 South Tryon Street
Suite 1780
Charlotte, North Carolina 28281
(704) 358-4838
www.asrisk.com

Lowers & Associates
125 East Hirst Road, Suite 3C
Purcellville, VA 20132
540-338-7151
www.lowersrisk.com

Brinks US
555 Dividend Drive
Coppell, TX 75019
www.brinks.com

Should you wish to join ATMIA's ATM Software portal on www.atmia.com, e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com

Disclaimer

The ATM Industry Association (ATMIA) publishes this best practice manual in furtherance of its non-profit and tax-exempt purposes to enhance the security of ATM software security. ATMIA has taken reasonable measures to provide objective information and recommendations to the industry but cannot guarantee the accuracy, completeness, efficacy, timeliness or other aspects of this publication. ATMIA cannot ensure compliance with the laws or regulations of any country and does not represent that the information in this publication is consistent with any particular principles, standards, or guidance of any country or entity. There is no effort or intention to create standards for any business activities. These best practices are intended to be read as recommendations only and the responsibility rests with those wishing to implement them to ensure they do so after their own independent relevant risk assessments and in accordance with their own regulatory frameworks. Further, neither ATMIA nor its officers, directors, members, employees or agents shall be liable for any loss, damage or claim with respect to any activity or practice arising from any reading of this manual; all such liabilities, including direct, special, indirect or inconsequential damages, are expressly disclaimed. Information provided in this publication is "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement. The name and marks ATM Industry Association, ATMIA and related trademarks are the property of ATMIA.

Please note this manual contains security best practices and should not be left lying around or freely copied without due care for its distribution and safekeeping.

US REGIONAL SPONSORS – MARCH 2011

GLOBAL SPONSORS – MARCH 2011

Table of Contents

CIT Carrier Best Practices – ATM Cash Risk Mitigation

Protecting the cash that funds your ATM program is paramount for every ATM deployer. ATM cash differences, thefts, and losses can quickly erode the profitability of an ATM program, or worse, can threaten an ATM deployer's ability to continue operations. In recent years there has been a significant increase in cash thefts associated with cash-in-transit (CIT) carriers at their vaults, in transit, and even after the funds have been loaded into the ATM. In 2010 alone, there were numerous transit losses including: a high-profile theft where a carrier's owner stole tens of millions of dollars out of their own vault, a bold robbery of a carrier vault which resulted in a loss of millions, and numerous bill denomination frauds netting hundreds of thousands of dollars that may have been prevented by the carrier using stronger processes while servicing the ATMs. Some of these losses were covered by insurance, but many found no coverage. In total, these losses have created significant pricing pressure on cash in transit insurance which is impacting armored carriers, banks and independent ATM deployers alike.

Selecting a quality CIT carrier can be one of the best ways to minimize the risk inherent in the ATM business as well as to reduce insurance costs. Thorough upfront and ongoing reviews of CIT carriers can help reduce the risk of theft by spotting weak points at the carrier and proactively addressing them. We must continually evaluate the due diligence process and update the requirements based on patterns of past thefts and potential means of future thefts.

The methods CIT carriers use to manage their vault can have a huge impact on the security and insurability of the cash. Carrier offices with sound operating procedures and security are best positioned to respond quickly and appropriately as issues arise.

These are best practices, and may not be applicable to all carriers. It is understood that not all carriers will be able to follow all of these recommended best practices. In some instances, there may be mitigating circumstances that can help alleviate concerns for customers and cash providers. As banks and independent ATM deployers evaluate new and existing CIT carrier relationships the following best practices should serve as a guide.

1. Insurance Requirements

- All Risk Armored Carrier insurance policy including employee dishonesty/fidelity coverage. Limits should be equal to at least the amounts stored "on-premise" and/or "in transit."
- Commercial General Liability insurance policy including premises/operations, products/completed operations, personal injury, blanket contractual liability and umbrella coverage with limits of at least $1,000,000 per occurrence and $5,000,000 in the aggregate.
- Commercial Automotive insurance (including uninsured and underinsured) covering personal injury and property damage with combined limits of at least $1,000,000 per occurrence.
- Workers Compensation insurance policy covering all employees to at least $1,000,000 – in many cases, limits will be statutory.
- All insurances should be with an insurer with an A.M. Best Rating of A, Class VIII or better.

2. External Audit Requirements

- In addition to internal audits and cash provider initiated audits, an annual cash audit (involving an appropriate representative sample, if not all carrier locations completed as unannounced random audits) is completed by an approved independent third party to include a full cash count and reconciliation of all inventories, with confirmations sent out to each customer/inventory holder and tracked for responses. A summary report is to be sent out once complete to all designated parties.
- With the cash audit, a survey component should be included that, at a minimum, involves a review of the internal controls surrounding cash handling. A summary report of controls and deficiencies should be produced at least annually for designated parties.

3. Personnel Screening and Training

- A pre-employment screening process is in place that consists of a criminal history and credit history check going back seven years, drug and alcohol testing, and polygraph testing (if prohibited by law, psychological testing should be substituted).
- Training is in place for vault, cash services, route, and opening/closing personnel, as well as branch access controllers.
- All personnel undergo emergency situation training and assault reaction training.

4. Access Controls

4.1. Opening/Closing Procedures

- No one person alone has access capability to primary liability storage area/vault. The employees who have the necessary access devices to open the primary liability storage do not come together until both the facility exterior and interior have been cleared. The vault must require dual control to open.
- Opening procedures are done any time a branch is reopened after being closed.
- Other employees are not permitted on site until the conclusion of the opening procedures, unless they are part of the opening team.
- A duress feature is available on the alarm keypad and known by all opening/closing employees.
- Portable hold-up alarm and/or communication devices are carried by all opening/closing employees.
- Management (outside of the opening/closing crews) performs a review monthly of the opening/closing procedures to ensure all steps are performed as required. This review is documented.

4.2. Terminal and Liability Access Devices

- An analysis is done at an appropriate frequency to ensure that no one person has too much access, unauthorized or unnecessary, to either the terminal or liability storage. This documented review also ensures the proper accountability and control of these devices.
- Keys/cards providing access to the terminal, restricted areas, and containers for restricted access devices and liability storage, are recorded in a master register. Master registers are controlled.
- Terminal keys/cards are formally issued, with the date, issuer, person issued, along with a statement in the receipt outlining the responsibilities of the person issued to safeguard the device.
- Terminal keys/cards are tagged (tamper evident) or marked for identification and accountability.
- All keys/cards providing access to the terminal, restricted areas, and containers for restricted access devices and liability storage, are inventoried on a monthly basis under dual custody and notification immediately if not found. This is documented.
- Exterior terminal access locks are routinely changed annually, or sooner as needed.
- Non-issued keys/cards for terminal, restricted areas, and containers for restricted access devices and liability storage, are secured in a container requiring dual control, with the use of dual locks or dual trackable seals, for access or secured in a tamper evident bag and stored in the vault, and accounted for. Note: Keys

of this nature should always be stored under dual control; CCTV can not be used to achieve dual control. The only exception is for storing keys that do not involve dual control access; these should be controlled by an authorized key user.

- Vault/safe combinations are issued in a manner to require dual control access to liability storage. Exceptions may be granted for e-cash storage based on the liability amount and type of locking device, provided insurance is in place for such procedure.
- A procedure is in place to open the vault without compromising dual control if someone calls in sick or is unable to be present.
- If a vault combination must be written, it is encrypted. No written vault combination is kept on site.
- The vault/safe combinations are formally issued with the date, issuer, person issued, along with a statement in the receipt outlining the responsibilities of the person issued to safeguard the device.
- The alarm system is kept current with users. Terminated employee codes are removed within 24 hours.
- Alarm codes are unique to each individual.
- Alarm codes are formally issued with the date, issuer, person issued, along with a statement in the receipt outlining the responsibilities of the person issued to safeguard the device.
- If an alarm code must be written, it is encrypted. No written code is kept on site.
- The alarm codes are routinely changed annually, or sooner as needed.

4.3. General Access Controls

- Stationary alarm system hold-up devices are located in the manager/administration office, all liability handling areas (not including storage), and at the facility vehicle doors.
- Portable alarm system hold-up and/or communication devices are worn at all times by at least one manager on duty and one designated person in the liability handling areas.
- Mantraps are at all key entry points.
- Branch entry is restricted to one person through the mantrap at a time.
- Access through the mantrap is remotely controlled from a secure area. A CCTV monitor is used if there is no direct visibility.
- Access through a mantrap for visitors is granted only after an employee has verified the identity of the person and searched any items carried by that person.
- If there is no prior branch notice, the auditor is validated at a higher company level outside the branch.

- Vault/safe/liability cage and container access is recorded in a register, showing the date, time, seal number, and the signatures of the two persons involved.
- Visitors (to restricted areas) are recorded in a register, showing the date, time, along with the escorting person.
- All company personnel and visitors, and their belongings, while on company property, are subject to search.
- When no vehicle trap is installed, a guard is present whenever the vehicle door is opened and is in reach of a hold-up alarm device. The guard is positioned on the outside prior to the door opening and until the door is closed. A company person is used, even for non-company vehicle access.
- Non-company vehicles given access into the terminal are searched by company personnel on the outside of the facility or in a vehicle trap. The search should not expose the vehicle crew or cargo to external attack.
- All vehicles are cleared prior to being granted access inside the terminal.

5. Vault

- All liability movements are properly controlled through and receipted in and out of the vault.
- A piece by piece verification, along with an inspection for bag integrity is performed during each check-in/out for all liability under dual custody. This is documented with the signatures of the people involved.
- Liability checked out/in is in containers/bags with a tamper evident seal
- The vault check-in procedure ensures accountability for all liability and pertinent documentation.
- Consolidated liability is prepared and sealed under dual control. This is documented.
- The vault department maintains adequate control over the liability within the department and under the signature custody of the department to prevent unauthorized access from non-department personnel.
- Vault personnel are armed or have access to weapons while in their department to react to an armed assault.
- Documented self-audits must be completed at least monthly by management outside of the direct oversight for this area.
- Vault area must be manned by two people at any time liability is exposed.

6. Cash Services

- Customer inventories are balanced under dual custody daily. The signatures on the counting and mathematical balancing documentation of the two people involved attests to this procedure. All e-cash associated with the inventory is included in the reconciliation and physically counted (counted at least once a week if in transit). The physical count should be blind.
- Within the vault/safe cash must be segregated by customer.
- Within the vault/safe cash inventories must be accessed under dual control. Dual control should be physically required and not limited to procedural.
- Customer inventory containers are further secured with a seal on/off procedure and an access log.
- A perpetual customer inventory log should be maintained noting by denomination all additions or removals of cash.
- The access register should note audits by internal staff and external auditors.
- An emergency cash activity log is used to show all emergency cash movements in and out of the safe/container by customer.
- E-cash is bagged and labeled separately.
- Liability handling and processing is done under dual control.
- The cash services department maintains adequate control over the liability within the department and under the signature custody of the department, to prevent unauthorized access from non-department personnel.
- If ATM residuals are not recycled, re-deposits are done within two days.
- Random audits are performed by management, outside of the direct oversight of this area, of the customer inventory accounts. At least one currency account is done monthly. This is documented.
- Tellers know where the stationary hold-up alarm devices are located.
- Ample video coverage should be identified in all open liability areas.

7. Transit

- Liability must be picked up in an armored vehicle by armed employees in uniform.
- The route crew complement must be a minimum of two-person. An exception for a one-person route may be warranted based on unique vehicle and crew protection systems employed.

- Armored vehicles are used for cash transport. Exceptions may be given for less than $100,000 (if the insurer has a rider for non-armored). Vehicles should meet a minimum of UL Level 3 for the cab and cargo compartments.
- Vehicles are loaded in a secure environment.
- An over-the-pavement policy is established and monitored.
- Vehicle to vehicle transfers done outside of protected areas are adequately controlled.
- Random unannounced surveillance is performed on each route person twice annually. This is documented.
- Site security surveys are done by each route quarterly, appropriately managed, and documented as such.
- A master register accounting for all vehicle keys (active/spare) is maintained.
- Vehicle keys are issued and returned daily through a receipting process.
- All vehicle keys are inventoried monthly under dual custody. This is documented.
- All vehicle keys are secured in a container requiring dual control, with the use of dual locks, for access; or secured in a tamper evident bag and stored in the vault, and accounted for; or placed in a controlled area that is covered by CCTV to the extent that the removal of the keys can be seen.

8. ATM

8.1. General Controls

- Personnel are rotated at least once every three months or a documented monthly random ATM cash audit program is in place where an audit is performed on a machine for each servicer.
- ATM variances are monitored daily. Audits are done as appropriate to resolve variances.
- System access codes for ATMs are changed when the company takes them over. These codes are changed annually at a minimum, or more frequently when needed such as with an employee termination or change in position.
- Pass codes should NEVER be written in or on the ATM in any manner.

8.2. Traditional Spin Dial Lock ATMs

- ATM safe combinations should not be written in the clear when issued to personnel.

- Combinations, if stored on site (paper), are encrypted, kept in a container requiring dual control, with the use of dual locks, for access. The container is kept secure when not in immediate use.
- Combinations on traditional spin dial ATMs are changed annually at a minimum, or more frequently when needed such as with an employee termination or change in position.
- Combinations on the ATMs are changed when the company takes them over.
- Both unique and generic ATM alarm codes are controlled and secured in a container requiring dual control access, with the use of dual locks, if maintained at the branch and not permanently issued.
- ATM alarm codes, if issued and written down, are encrypted and, if not permanently issued, are issued to and from the route crew member.
- Non-generic keys are itemized on a master register.
- Non-generic keys are checked in and out on a daily basis.
- Non-generic keys should be audited monthly under dual control with the results documented.
- Non-generic keys are secured in a container requiring dual control, with the use of dual locks, for access; or secured in a tamper evident bag and stored in the vault, and accounted for; or placed in a controlled area that is covered by CCTV to the extent that the removal of the keys can be seen. Note: If the branch services traditional spin dial lock ATMs, keys of this nature should always be stored under dual control; CCTV can not be used to achieve dual control.

8.3. Non-static combination ATMs

- Electronic keys are itemized on a master register.
- Electronic keys are receipted for if permanently issued, formally issued and returned if not permanently issued.
- Electronic keys are inventoried monthly under dual custody. This is documented.
- "R" and "F" Electronic keys (if not maintained by the person issued) are secured in a container requiring dual control, with the use of dual locks, for access or secured in a tamper evident bag and stored in the vault, and accounted for. Note: Keys of this nature should always be stored under dual control; CCTV can not be used to achieve dual control.
- Electronic combinations (Company Route/FLM personnel) provided orally to routes are strictly controlled with authentication of the person requesting.
- The individuals who issue combinations have no access to ATM access devices.

- If a close seal is not obtained or if the seal number provided does not confirm the ATM is secure, immediate action is taken to confirm the machine is actually locked.
- ATM access information obtained and provided electronically is adequately protected from unauthorized personnel.

9. Physical Security

9.1. CCTV

- Video storage is kept for a minimum of 90 days.
- CCTV camera coverage includes, at a minimum, all terminal access points, and liability storage and handling areas.
- The recording speed is set as appropriate to provide quality video playback; three to four frames per second is recommended.
- Recording devices are all operational and checked monthly, documented by signature.
- Recording devices all have the correct date and time.
- Recording devices/media are secured from unauthorized access and those persons under surveillance.

9.2. Terminal Design

- Exterior walls, ceilings, and floors (where applicable) are constructed with materials to resist attack.
- No windows exist, unless they are reinforced to the same degree as the exterior wall requirement.
- Exterior doors, to include mantrap inner and outer doors, provide a minimum of BR UL Level 1 protection.
- Emergency exit doors are on 24-hour alarm protection, have panic hardware with a local audible device, and no hardware exists on the exterior of the door other than a lock plate.
- Mantrap walls and ceiling are reinforced to the same degree as the exterior wall requirement.
- The mantrap doors are interlocked or the opening of both doors causes a local alarm to activate.
- The vault entrance is surrounded by a hardened anteroom.
- Cargo turn-in bays (mantraps) are used and provide protection from access to the vault anteroom.
- Terminal vehicle doors provide adequate protection. Consideration is taken for the type of facility.

- When a vehicle trap is not used or if the vehicle trap doors are not interlocked, an audible or visual signal is in place to alert staff that a vehicle door is open.
- The interior of the terminal has barriers and locked doors to control personnel movement and prevent unauthorized access to liability handling and storage areas.
- Facility access devices/locks are high security and allow for unrestricted egress. "Fail safe" electric locks are not used.
- An intercom system is installed near the outer entrance door for communications with persons controlling access to the facility.
- All entrances/exits, and liability storage and handling areas have adequate emergency lighting which is tested monthly, with the results documented.
- Perimeter lighting is in use during non-daylight hours and adequately supports the CCTV cameras.
- The terminal is surrounded by a fence with a minimum height of eight feet and a distance of 20 feet from the outer branch wall to the fence line. Access through the fence gate is adequately controlled.
- Any openings greater than six inches are reinforced to the same degree as the exterior wall requirement.

9.3. Alarm Systems

- The premises system is supported with a current UL certificate indicating:
  - Central Station Monitoring
  - Extent 2 Protection
  - Standard Line Security
- The vault/safe system is supported with a current UL certificate indicating:
  - Central Station Monitoring
  - Complete Protection
  - Standard Line Security

9.4. Liability Storage

- Vaults/safes meet the following requirements: Note: Liability is only stored in an appropriate container when unattended.

Liability Storage Amount	UL Rating
Up to $50,000	TL-15
$50,000.01 to $200,000	TRTL-15X6
$200,000.01 to $250,000	TRTL-30
$250,000.01 to $1,000,000	TRTL-30X6 or Class I Vault
$1,000,000.01 +	TRTL-60X6 or Class II Vault