

NCR ATLEOS

October 2026

# ATM Fraud:

A customer-focused guide to the principal forms of ATM fraud and the layered measures available to reduce risk.

NCR ATLEOS

October 2026

# ATM Fraud:

A customer-focused guide to the principal forms of ATM fraud and the layered measures available to reduce risk.

## Table of contents


1. Introduction ..... 2
   1.1 Understanding ATM fraud ..... 2
2. Card crime ..... 4
   2.1 Skimming ..... 4
   2.2 Shimming ..... 4
   2.3 PIN capture ..... 4
   2.4 Card trapping ..... 5
   2.5 EMV Relay ..... 5
3. Cash crime ..... 6
   3.1 Cash trapping ..... 6
   3.2 Transaction reversal fraud ..... 6
4. Unauthorised cash dispense and HBA ..... 7
   4.1 HBA at a glance ..... 7
   4.2 Why HBA matters ..... 8
   4.3 Deployment considerations ..... 8
5. Layered security ..... 9
   5.1 Contactless opportunity ..... 9
   5.2 Removing the prize ..... 9
6. Recommendations ..... 10

About NCR Atleos ..... 11


©2026 NCR Atleos. All rights reserved.

# 1. Introduction

ATM fraud targets the cardholder, the card, the transaction or the cash-dispense process. Methods range from card skimming and PIN capture to cash trapping, transaction reversal, EMV relay and attempts to trigger cash dispense without proper approval. Criminal techniques continue to shift as solutions are introduced, so ATM security needs to be adaptable as well as layered.

**There is no single solution that removes ATM fraud risk**. The strongest approach protects the full transaction: card entry, PIN entry, ATM software, host approval, cash dispense and the operational processes around the estate.

**KEY MESSAGE**
Protect the complete customer transaction, from card and PIN entry through to host approval and cash delivery.

## 1.1 Understanding ATM fraud

ATM fraud differs from a forced physical attack on the safe. It seeks to exploit the customer interaction or transaction process to obtain physical cards, card data, PIN or cash. Logical attacks can overlap with fraud where an attacker attempts to manipulate the ATM environment to trigger cash dispense.

The practical risk is different for every estate. For example:

- Location
- ATM design
- Customer behaviour
- ATM software
- Host policy
- Local criminal activity

These things all shape exposure. A single global view is not enough; risk should be assessed by estate, deployment type and local attack pattern.

Estate risk is also shaped by how visible the ATM is, how often it is serviced and how easily a criminal can interact with it without being challenged.

©2026 NCR Atleos. All rights reserved.

| ATM Location | Location Characteristics |
|---|---|
| Drive Up ATMs | Unattended, freestanding, front access, larger cash capacity. |
| Off premise – lobby | Unattended, freestanding, front access. |
| 24hr Unattended Lobby (Vestibule) ATMs | Unattended, Through the Wall (TTW), rear access. |
| Branch Through the Wall ATMs | Unattended, Through the Wall, rear access. |
| Branch on Premise ATMs | Attended, freestanding or Through the Wall, front or rear access. |

**THREAT MOVEMENT**
When one route becomes less attractive, criminals often move to another attack point, deployment type or market.



©2026 NCR Atleos. All rights reserved.

# 2. Card crime

## 2.1 Skimming

Skimming captures magnetic-stripe card data during a genuine customer transaction. The stolen information is normally combined with the customer's PIN and used where magnetic-stripe transactions or fallback remain available.

Skimmers may be positioned at the front of the card reader, concealed deeper inside it or connected elsewhere in the ATM environment. Because the attack surface extends beyond the visible fascia, protection should cover the full card-data path.

Contactless authentication can reduce these opportunities because the card remains in the customer's possession.

| Attack area | Customer impact | NCR Atleos Solution |
|---|---|---|
| Fascia skimming | Card data can be captured at the card-entry point. | Skimming Protection Solution (SPS) and SPS2 help protect the reader entry area. |
| Deep insert skimming | A concealed device inside the reader may be difficult to identify visually. | Skimming Surveillance Solution (SSS) and Tamper Detecting Card Reader (TDCR) support detection. |
| Internal data path | Attackers may target card data elsewhere in the ATM environment. | Tamper-resistant readers, encrypted communications and logical security provide layered protection. |

## 2.2 Shimming

Shimming targets chip-card communications rather than the magnetic stripe. While EMV makes conventional cloning harder, captured chip-communication data may still support fraud attempts where fallback, issuer validation gaps or relay-style misuse are present. This is why shimming should be treated as part of the wider card-data protection model, not as a separate niche risk.

## 2.3 PIN capture

Card-data attacks usually need the corresponding PIN. Concealed cameras, keypad overlays and shoulder-surfing can all be used to capture it. PIN shields, routine

©2026 NCR Atleos. All rights reserved.

inspection, staff awareness and customer education remain important prevention measures.

## 2.4 Card trapping

Card trapping deliberately prevents the customer's card from being returned. Contactless authentication can reduce these opportunities because the card remains in the customer's possession.

## 2.5 EMV Relay

An EMV relay attack attempts to use a genuine chip or contactless interaction to support a fraudulent transaction elsewhere. The card is not copied in the traditional way; the genuine card data is transmitted in real time from the victim card/ATM through a series of nodes in a network to a card simulator device or criminal phone which presents the genuine card data to the cash out ATM.

- This distinction matters because relay is not solved in the same way as traditional skimming. Contact and contactless EMV relay need to be considered across the wider payment environment, including unattended terminals outside the ATM channel. NCR Atleos ATM software supports EMV relay prevention at the ATM terminal, with issuer monitoring and transaction analytics forming part of the broader response.

**IMPORTANT DISTINCTION**
Skimming captures reusable magnetic-stripe data. Relay attacks misuse a live interaction with a genuine card or device.



©2026 NCR Atleos. All rights reserved.

# 3. Cash crime

## 3.1 Cash trapping

Cash trapping prevents a customer from receiving notes that have been presented by the ATM. The customer may believe the transaction has failed, allowing the criminal to return later and recover the cash. Attacks can target the external cash exit (External Cash Trapping) or the internal presentation path (Internal Cash Trapping).

Type 1 – External Cash Trapping: A fake shutter attack is one where an attacker will place an overlay on the ATM fascia that covers the cash exit shutter and is disguised to look like a cash exit shutter. When a cardholder requests a cash withdrawal, they are then unable so see the cash presented by the ATM and will be tricked into thinking that the ATM has failed to dispense. When the cardholder leaves, the criminal returns to remove the overlay and retrieve any cash trapped behind it, resulting in the customer being debited and potentially raising a claim.

Type 2 – Internal Cash Trapping: An attack typically mounted against belt driven cash dispensers. A device such as a 'cash claw' or 'fork' is inserted into the presenter module during a staging transaction. The next transaction cash bundle becomes jammed in the device such that it cannot be dispensed or purged. The attacker then breaks open the shutter to remove the device and cash.

NCR Atleos solutions address both forms of cash trapping by helping to reduce customer impact and lower the administration burden on cash claims team. The right response depends on the ATM model, cash-delivery mechanism, application behaviour and local attack pattern.

## 3.2 Transaction reversal fraud

Transaction reversal fraud (TRF) is a category of fraud not one specific attack type. TRF means an attacker deliberately induces a fault during a cash dispense operation such that the ATM software sends a reverse message to the host, while the attacker has removed some or all of the dispensed bills. This results in no debit to the cardholder account. TRF attacks are typically executed using a stolen, prepaid or skimmed card to disguise attacker identity. Attackers will often repeat the attack multiple times, which is possible because no funds are debited from the account. Therefore, the account doesn't run dry and daily withdrawal limits are not breached.

As well as manipulation of the reversal policy, criminals may also introduce physical elements to the crime that involves damage to the ATM. Ensuring the ATM Software is up to date alongside correct mapping of automatic reversals to NDC messages is critical. Strong host reversal policies, transaction monitoring and cash-dispense integrity  are key to reducing exposure.

©2026 NCR Atleos. All rights reserved.

# 4. Unauthorised cash dispense and HBA

Host Based Authentication, also known as End-to-End Cash Authentication (E2EA) as defined in CEN XFS 3.50 CDM Standard, provides an additional defence against logical attacks that attempt to trigger unauthorised cash dispense. It creates a trusted link between host authorisation and the cash dispenser (including recyclers), without relying on ATM software executing on the compute device (including the ATM application), to determine whether a dispense instruction is authentic. This puts the decision-making trust regarding cash movement in known cryptographically and physically secure locations i.e. the dispenser firmware in the safe and the authorising host in a data centre.

Removing this trust from the compute device and any software executing on it means that any manipulation made to the core or it software will have no ability to issue cash movement commands to the dispenser, as the dispenser cannot cryptographically authenticate these commands therefore eliminating all jackpotting type attacks.

## 4.1 HBA at a glance

| Stage | What happens | Customer benefit |
|---|---|---|
| Issuer Host approval | Issuer approves the withdrawal as today. | Establishes single source for dispense authorisations. |
| Protected instruction | Acquirer host generates cryptographical secure dispense token. | Helps prevent unauthorised or altered instructions. |
| Dispenser validation | The cash dispenser confirms the instruction is valid. | Cash is released only after successful validation. |
| Confirmed outcome | The transaction outcome is securely returned. | Supports oversight and reconciliation. |

©2026 NCR Atleos. All rights reserved.

## 4.2 Why HBA matters

- Adds independent validation at only secure and trusted solution elements (Dispenser Firmware and Acquirer Host).
- Removes all trust from ATM software executing on the compute device for cash movement.
- Complements existing black-box protection, software hardening and secure communications.
- Supports a broader end-to-end approach to transaction security.
- Eliminates all Jackpotting type attacks.

## 4.3 Deployment considerations

HBA spans the host, ATM software, cash dispenser (including recyclers) and the processes used to manage trusted communication. Financial institutions should assess estate readiness, platform compatibility, key management processes, operational continuity, service processes and resilience when planning adoption.

NCR Atleos can support financial institutions in assessing how HBA fits within existing and future ATM estates. The appropriate path will depend on the ATM portfolio, host environment and operating model.

**HBA OUTCOME**
Cash is released only when the dispense instruction can be linked to valid host approval.

.



©2026 NCR Atleos. All rights reserved.

# 5. Layered security

A strong ATM fraud strategy deals with today's attacks while reducing the value of the target over time. Each layer should work with the others, so that a weakness in one area does not expose the full transaction.

The table below brings the main fraud areas together into a single view, showing how each threat family maps to a practical security response.

| Threat family | Examples | How to prevent the attack |
|---|---|---|
| Card crime | Skimming, shimming, card trapping, EMV Relay and PIN capture | Skimming requires protection across the full card-data path through SPS, SPS2, SSS and TDCR, combined with PIN protection and reduced reliance on reusable magnetic-stripe data.<br>EMV relay protection requires maintaining the latest ATM software, with issuer monitoring and transaction analytics across the wider payment environment. |
| Cash crime | Cash trapping and transaction reversal | Cash-exit and presenter protection, supported by the latest ATM software and correct mapping of automatic reversals to NDC messages. |
| Unauthorised cash dispense | Logical and black-box attacks | Layered logical security with Host Based Authentication (HBA) linking cash delivery to valid host approval. |

## 5.1 Contactless opportunity

Contactless EMV reduces the need to insert a physical card. That can reduce opportunities for card trapping, card-ejection distraction and magnetic-stripe capture at the reader. It still needs to sit alongside issuer measures, relay monitoring and clear customer communication.

## 5.2 Removing the prize

The strongest long-term move is to reduce what the attacker can gain. For card fraud, that means reducing reliance on reusable magnetic-stripe data. For unauthorised dispense, it means linking cash delivery to valid host approval.

**KEY MESSAGE**
Layers work together. No single measure protects the full transaction on its own.

©2026 NCR Atleos. All rights reserved.

# 6. Recommendations

The following actions reflect what NCR Atleos sees working across live estates. They are ordered so that the highest-impact, lowest-effort measures come first, and they should be applied in line with estate profile, deployment type and local attack patterns.

| Focus area | Recommended action |
|---|---|
| Inspection and response | Make routine inspection and incident response standard practice, so suspicious changes are found and acted on quickly. |
| Estate prioritisation | Address the highest-risk ATMs first, based on location, design, configuration and local attack patterns. |
| Unattended sites | Apply closer oversight where footfall is low and deep insert attacks are more likely. |
| Card reader protection | Reduce exposure across the full card-data path, not only the visible fascia. |
| Software maintenance | Keep ATM software, operating systems and dispenser platforms current and supported. |
| Cash trapping | Protect both the cash exit and the presenter against the forms of trapping seen locally. |
| Transaction reversal | Control exposure through host reversal policy, correct message mapping and transaction monitoring. |
| EMV relay | Ensure ATM software is kept up to date and the protection enabled. |
| Magnetic stripe | Move away from magnetic-stripe reliance, using EMV-only and contactless options where practical. |
| Host Based Authentication | Assess where HBA fits, particularly where cash dispense needs stronger linkage to valid host approval. |

**CLOSING VIEW**

ATM fraud is best addressed as a connected security problem, not a set of unrelated attacks.

©2026 NCR Atleos. All rights reserved.

# About NCR Atleos

NCR Atleos (NYSE: NATL) is the leader in expanding self-service financial access, with industry-leading ATM expertise and experience, unrivalled operational scale including the largest independently-owned ATM network, always-on global services and constant innovation. NCR Atleos improves operational efficiency for financial institutions, drives footfall for retailers and enables digital-first financial self-service experiences for consumers. NCR Atleos is ranked #12 in Newsweek's prestigious 2025 Top 100 Global Most Loved Workplaces® list. NCR Atleos is headquartered in Atlanta, Ga., with approximately 20,000 employees globally. For more information, visit www.ncratleos.com.

©2026 NCR Atleos. All rights reserved.