INETCO SOLUTIONS SHEET

INETCO Solutions for ATM Cash-Outs and Early Warning Fraud Detection

Notifying you when terminals, cards or transaction switches are under attack

Organized crime syndicates are targeting payments systems, exploiting software and process vulnerabilities to bypass or remain undetected by traditional fraud defense systems. INETCO solutions will enable you to limit your risk and financial exposure by adding a new layer to spot threats earlier and react faster.

Immediately spot Advanced Persistent Threats (APTs) that often go undetected by traditional risk monitoring systems:

- Know when a transaction enters a payments switch, but never leaves for authorization
- Be immediately alerted to repeat card usage at the same terminal, or across an unlikely geographical area
- Watch for anomalous patterns such as multiple cards used in sequence at the same terminal

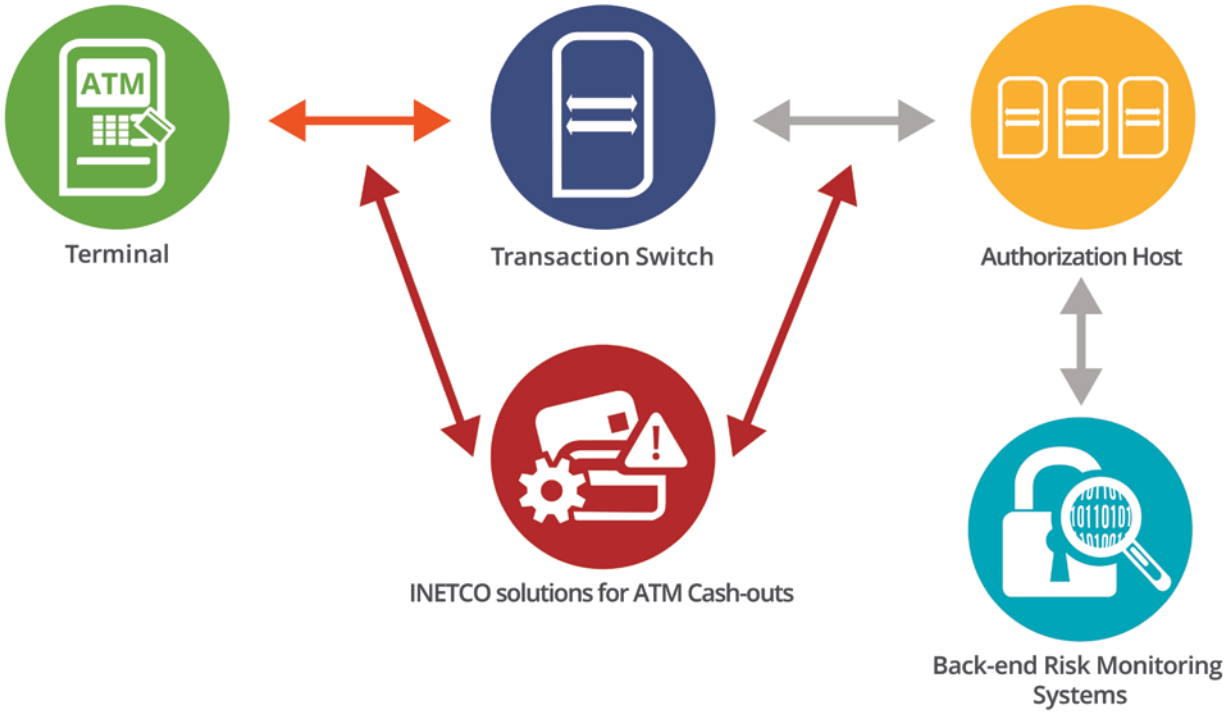

DIAGRAM 1 – Risk monitoring systems that reside on the back-end of your payments system cannot easily identify when attacks occur on the front-end. With the ability to correlate front-end and back-end transactions, INETCO solutions for ATM Cash-outs and early warning fraud detection will help you quickly identify transaction behavioral anomalies and compromises to the payments switch.

Where the INETCO solutions help

Discover compromised cards that are not on your hot card list yet

Skimmed cards are typically used for a bunch of transactions in a row, coordinated across multiple devices, as criminals try to do as much damage as possible before the card can be flagged and various hot card lists get updated.

INETCO solutions look for this kind of rapid, repeat card usage and notify you immediately so you can take action. Thresholds can be set based on key variables such as card type, transaction values, and location to minimize false positives.

SUPPORTING FEATURES:

- **Real-time alert on repeat card usage over short time**
- **Real-time notification when distance between two consecutive transactions with the same card is not physically possible or likely**
- **Set different thresholds based on BIN ranges and geographies**
- **Receive notification when an excessive number of issued cards is carrying out withdrawals on foreign terminals within a specified time interval**
- **Identify when there is an abnormal number of foreign cards completing withdrawals on one or more of your terminals**

Pinpoint vulnerable terminals and devices

Criminals will often target specific devices or locations for coordinated attacks and exploit flaws in the equipment, cards, or geographical characteristics that make their attacks more successful

INETCO solutions detect anomalous transaction activity at the terminal level immediately, so you can investigate suspect terminals. Thresholds can be set differently based on terminal type, manufacturer, and location to detect rapid, repeat transactions, fallbacks to magstripe at EMV-capable terminals, excessive reversals, and transactions occurring outside normal business hours.

SUPPORTING FEATURES:

- **Real-time alert on repeat terminal usage over short time windows**
- **Set different thresholds based on terminal type, manufacturer and location**
- **Real-time alert on specific response codes and transaction fields (e.g. EMV capable card falling back to magstripe at EMV capable terminal)**
- **Set business hours for each device**

Know when your payment switch has been compromised

Specially crafted malware can cause your payment switch to authorize transactions locally instead of dispatching them to back-end fraud and authorization systems for evaluation. This malware is often designed to support card skimming or coordinated withdrawal attacks.

INETCO solutions detect these front-end attacks by tracking transactions at the network level, and looking for transaction requests that enter the switch, but never exit into back-end systems.

SUPPORTING FEATURES:

- **Multi-point monitoring to independently audit the end-to-end journey of every transaction from the network in real-time**
- **Multi-hop, multi-protocol correlation to immediately know when a front-end ISO transaction is not married with a back-end database transaction**
- **Real-time alerts on transactions that do not follow your conventional authorization path**
- **Immediate notification of unexpected stand-in behavior**

For more information on INETCO solutions, contact sales@inetco.com