# ATMIA Information Alert: Unlimited Operations (ATM Cash-Out)

Produced by the ATM Industry Association

Contributor:

Douglas Russell, Director, DFR Risk Management Ltd.

## Copyright Information

**e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com**

## Disclaimer

The ATM Industry Association (ATMIA) publishes this *ATMIA Information Alert: Unlimited Operations* in furtherance of its non-profit and tax-exempt purposes to promote information and best practices around payment 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 discussion paper; 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 discussion paper contains confidential information and should not be left lying around or freely copied without due care for its distribution and safekeeping.**

## GLOBAL SPONSORS

ACCESS CASH
atm marketplace
AURIGA the banking e-volution
ca$h N go ATM Network
CARDTRONICS
Diebold Nixdorf
dpl
esq
Euronet WORLDWIDE
FUJITSU
GRG Banking We Move Faster
HITACHI
HYOSUNG
KAL ATM Software
mastercard
NCR
OKI Open up your dreams
PARABIT Enhancing Self-Service & Improving Security
Payment Alliance INTERNATIONAL
Perto
PROSEGUR
TMD security
VISA

# Table of Contents

## 1.1. Definitions

Unlimited operations, also known as ATM cash-out fraud, involves compromising a card issuer's authorization system to eliminate or inflate withdrawal limits.

Money mules perform transactions using specific cards to extract as much cash as possible over a short period of time. Card data from genuine cards are often obtained in the early phase of compromising the card issuers systems. Once the card data has been compromised it is transferred to the money mules to be re-encoded onto magnetic stripe cards prior to the cash-out phase being triggered.

Perpetrators also perform cash-out fraud when they identify a lapse in normal authorization procedures. This can include exploiting a period of stand-in-processing or a system upgrade, during which time normal authorization limits might be suspended.

Cash-out fraud has been known to involve high-volume withdrawals in multiple countries and regions almost simultaneously. In the absence of the assistance of an insider employee, spear phishing linked to malware is known to be used to gain access to the systems.

Unlike ATM jackpotting, unlimited operations fraud does not exploit vulnerabilities in the ATM itself. The ATM is used to withdraw cash after vulnerabilities in the card issuers authorization system have been exploited.

## 1.2. Established and Increasing Threat

Unlimited operations is not a new type of fraud. ATMIA published an alert in 2016 titled "ATM Cash-Out Fraud (Unlimited Operations)" following high value fraudulent ATM withdrawals in Japan targeting a South African bank and card issuer.

Recently there have been further similar attacks detected globally and a law-enforcement agency (FBI) have issued an alert to the US banking industry warning of possibly imminent future attacks.

## 1.3. Withdrawal Limits

Withdrawal limits are primarily the responsibility of the card issuer and are usually set based upon the type and risk profile of specific accounts linked to the card issued. Under normal circumstances, a cash withdrawal value limit is set per calendar day (or per 24hrs) and at a value that does not exceed the available balance or credit limit of the account.

ATM deployers may also set a local withdrawal limit at their ATMs to limit the amount of cash that can be dispensed by the ATM per transaction. Local ATM withdrawal limits generally are of little consequence to the card issuer beyond possibly inconveniencing their card holders should a low limit be applied. The local ATM limit, in practise, is equal to or less than the amount authorised by the card issuer during the transaction and so has little significance in managing the issuers risk.

## 1.4. Authorization Compromise & Money Mules

Unlimited operations / cash-out fraud incidents are successful when the perpetrators are able to overcome or inflate issuer withdrawal limits. In such circumstances, the local ATM withdrawal limit does become a limiting factor in the total value of funds that can be obtained by the 'money mules' enlisted to perform the fraudulent transactions.

Money mules are often quite separate from the sophisticated perpetrators that have compromised the issuers authorization system or identified a vulnerability in the procedures used for authorizing transactions at any given point in time. Money mules normally share a percentage of the total funds fraudulently obtained.

Local ATM withdrawal limits do vary from country to country and deployer to deployer. ATM deployers with relatively high local ATM withdrawal limits have previously been chosen to perform cash-out transactions.

## 1.5. Best Practices for Defending Against Unlimited Operations / Cash-Out Fraud

### Card Issuers

- Validate the security of the issuing and authorization systems against known cyber-attack vectors and compliance with industry standards and card scheme rules
    - Implement application whitelisting to block the execution of malware
    - Monitor for the presence of remote network protocols and administrative tools
    - Monitor for encrypted traffic (SSL or TLS) traveling over non-standard ports
    - Monitor for network traffic to regions wherein you would not expect to see outbound connections
- Set withdrawal limits to a value suitable to the type of account linked to the card
- Ensure adequate controls are in place to prevent unauthorized modification of card processing parameters such as withdrawal limits and geographic usage restrictions

  - Implement separation of duties or dual authentication procedures for account balance or withdrawal increases above a specified threshold
  - Monitor, audit and limit administrator and business critical accounts with the authority to modify the account attributes
- Monitor, alert and respond to suspicious activity such as high velocity, high value transactions
- Decline transactions on bank identification number (BIN) ranges and individual cards that are inactive including those that are not currently issued
- Verify full protection and fraud monitoring is maintained against cash-out fraud during stand-in processing (STIP)
- Inform law-enforcement partners when a breach has happened or been attempted

## ATM Deployers

- Surveillance of CCTV for multiple transactions being performed by a single individual
- Monitor, alert and respond to suspicious activity such as high velocity, high value transactions particularly related to cards from the same issuer
- Inform law-enforcement partners when an incident has been detected

# 1.6. Further Reading & Links

### ATMIA Best Practices

https://www.atmia.com/main/atmia-best-practices-library/

### ATMIA Fraud Alerts

https://www.atmia.com/education/security/fraud-alerts/