

An ATM Industry Association White
Paper



P.O. Box 4392
Biloxi, MS 39535
U.S.A.
+1 (228) 385-8806
www.atmia.com

Building Denomination Fraud Awareness A Guide to Prevention Techniques

*By Cynthia R. Habeeb, U.S. Manager and
ATMIA Denomination Fraud Committee*

Revised: February 2009

Contents

Contents	2
Introduction.....	2
Problem Statement.....	2
Previous Options.....	3
Industry Solutions	3
New Solutions.....	3
ATM Manufacturing.....	3
Challenge	3
Resolution	4
Processors	4
Challenge	4
Solution	4
ATM Service Organizations ...	5
Challenge	5
Solution	5
ATM Owners	5
Challenge	5
Solution	5
Communicate Responsibility	5
Assist Law Enforcement	5
Implementation	6
Summary	6

Introduction

In September 2006, Denomination Fraud became a pressing issue for the ATM industry. A large number of ATMs were in fact found to be still utilizing the manufacturer default pass code, resulting in a security weakness. These codes were in some cases available online.

Since then, new software, best practices and solutions have been made available to the ATM industry. This paper will detail ways of defending against Denomination Fraud.



Denomination Fraud occurs when an individual with ill intent obtains a management pass-code, accesses management functions and opts to change the denomination configured on the ATM to a lesser amount than required for the banknotes loaded in it. This enables the fraudster to withdraw more cash than is recorded as debited from the account. (See Figure 1, Sample Scenario of Denomination Fraud).

Problem Statement

Despite a brief decline in Denomination Fraud occurrences, a resurgence of this crime has occurred over 2008.

There are a few factors that contributed to this resurgence. One contributing factor was the difficulty in communicating the availability of

new security solutions to small ATM owners. The second contributing factor was the management of pass-codes. . Finally, catching a prosecuting the fraudsters have proven difficult.

Previous Options

Previously the primary option in protection against denomination fraud was centered on securing the ATM management pass-codes.

Industry Solutions

The ATM industry today has various solutions available to protect against Denomination Fraud.

New Solutions

As a result of the growing concern of denomination fraud that began in 2006 the ATM industry banned together to generate new solutions.

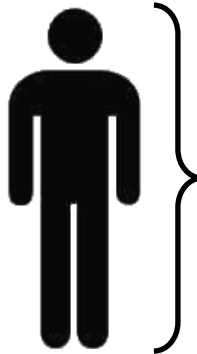
To define the solutions ATM manufacturers, processors, service organizations and ATM owners met together to determine realistic and suitable protective actions.

ATM Manufacturing

As with most secured devices there is always a manufacturer default pass-code. For the most part it is up to the owner to take on the responsibility to change the code and protect it.

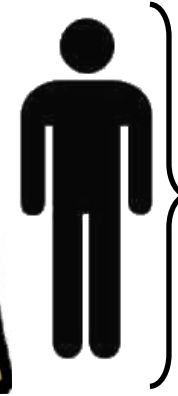
Challenge

Numerous ATM management pass-codes are not changed once in the field.



Individual obtains management pass-code through:

1. Web using manufacturer default pass-code.
2. Employment/ or an employee with an organization who utilizes this information.



Individual goes into management functions and changes Cassette A to reflect it is filled with '5's rather than '20's.



Individual requests a cash withdrawal for \$300 with a stored value card. The ATM will then dispense sixty (60) \$20 notes, allowing the individual to make \$900.

Figure 1
Sample Scenario of Denomination Fraud



ATM Industry Association (ATMIA)
website, www.atmia.com.

Resolution

Manufacturers have developed various software solutions forcing management pass-codes to be changed before accepting transactions. The majority of new ATMs already contain this software. To realize the full benefit of the software it is recommended that the latest version of software is installed on the ATM.

The new solution is incorporated in the latest version of software available for the majority of ATM models in the marketplace. Most manufacturers maintain the latest version of software on the password protected section of their respective website.

If you are unclear as to what version of software is housed on your ATM, please reference your owners manual. For more details regarding the software version and downloads please contact your ATM manufacturer.

ATM makes, model, and software versions may also be found on the password protected section of the

Processors

Rarely, if at all, do cash machine owners change the denominations available at an ATM.

Challenge

Create a solution that will automatically detect a change in the denomination amount programmed at the ATM.

Solution

Processors have a unique capability to detect unique occurrences with an ATM. As such writing special code to detect an oddity

is not necessarily a quick and simple task. Yet with those ATM terminals utilizing triton standard specifications an additional layer of security for ATM owners is more feasible.

To date there are a few processors who can now automatically shut down an ATM terminal when a denomination change is conducted at the terminal. Processors capable of this solution are referenced in this document.

Although this solution may create some inconvenience initially it takes only one,

ATM Manufacturer Contacts

Nautilus Hyosung

Mike Henson, Technical Support & Training Manager
Phone: (972) 350-7616
Email: mike.henson@us.hyosung.com

Tranax

Bill Dunn, Vice President, Retail ATM Sales Division
Phone: (972) 373-8600 ext. 203
Email: bdunn@tranax.com

Triton

James Phillips, Director N.A. Sales
Phone: (228) 868-1317
Email: james.phillips@triton.com



maybe two, incidents for the criminal to receive no reward and the fraud is stopped.

ATM Service Organizations

One of the most difficult processes for businesses is the hiring of the right employee for the right position.

Challenge

Employees utilize accessibility to management pass-codes to defraud an ATM.

Solution

Incorporate new procedures that take into account "Pass-code Destruction" policies for:

- ATM installations
- Service visits
- Cash Management visits

It is important to ensure that businesses are providing proper due diligence to prevent fraud.

ATM Owners

The liability for fraudulent activity ultimately falls on the ATM owner. Understanding the solutions available and steps to take in preventing fraud ultimately lies here.

ATM Processor Contacts

Cardtronics

Jerry Garcia, Chief Information Officer
Phone: (469) 237-3154
Email: jgarcia@cardtronics.com

Columbus Data

John Willmon, VP Business Development
Phone: (214) 276-5712
Email: jwillmon@columbusdata.net

Élan Financial Services

Steve Gernes, ISO Sales & Support Manager
Phone: (800) 343-7064
Email: steven.gernes@usbank.com

Switch Commerce

Roger Myers, President
Phone: (877) 550-1310
Email: rmyers@switchcommerce.com

Challenge

Communication of preventative measures, where to obtain necessary tools and general information to prevent Denomination Fraud.

Solution

Evaluate the options available from both manufacturers and processors to better secure your ATM. Implement changes to administrative and management pass-codes at your ATM. Whether an ATM owner changes pass-codes every quarter or sets new codes each

time a change is made in employees with access to information.

Communicate Responsibility

Incorporate new clauses into contracts to ensure all parties impacted understand responsibilities.

Oftentimes the party responsible for pass-code management is unclear. Ensure that contracts explicitly state the entity that is accountable for management code accessibility.

Assist Law Enforcement

Evaluate ways of assisting and educating law enforcement about the industry. Two-way information sharing is vital.



in protecting the ATM industry and consumer from fraudulent activity.

Implementation

Determine what features are accessible and evaluate the business' overall pass-code management process. Define a strategy and implementation process that best fits your business need.

Summary

Building awareness and communication of solutions and security best practices is paramount

THANK YOU TO ALL COMMITTEE PARTICIPANTS WHO ASSISTED IN THE DEVELOPMENT AND EXECUTION OF STRATEGIES TO PROTECT THE ATM INDUSTRY FROM DENOMINATION FRAUD:

Access To Money, AS Risk, Cardtronics, Columbus Data, First Data, Fiserv, Innovus, International Merchant Services, Kahuna Business Group, Mastercard, Metapay, Payment Alliance International, RBS Lynk, Solvport, Switch Commerce, Tranax, Triton and U.S. Bank

ATMIA U.S. REGIONAL SPONSORS



GLOBAL SPONSORS



ATMIA is an independent non-profit organization representing the whole ATM industry. Our mission is to protect the industry through international security best practices, present an accountable voice on major issues and produce annual events and training for our members in over 45 countries.