ATM SECURITY ASSOCIATION

ATM Security Association for Enhanced Technology

Operating Policies and Procedures

Version 1.0 2019-03-30

ATMIA

Education ♦ Advocacy ♦ Connections

Produced by the ATM Industry Association

Copyright Information

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

Disclaimer

The ATM Industry Association (ATMIA) publishes *ATM Security Association for Enhanced Technology Operating Policies and Procedures* to promote good governance and provide guidelines for ASA practices and procedures. 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

TMD security	KAL ATM Software	NCR	FIS	Perto	Euronet WORLDWIDE
atm marketplace	cash N go ATM Network	CARDTRONICS	mastercard	PROSEGUR	HYOSUNG
UnionPay 银联	MetaBank	HITACHI	esq	VISA	Diebold Nixdorf
PARABIT	dpl	ACCESS CASH	AURIGA	Payment Alliance INTERNATIONAL	FUJITSU
OKI Open up your dreams	GRG Banking				

Table of Contents

Foreword

The purpose of this operational manual is to provide guidelines for ATM Security Association (ASA) practices and procedures. Since governance of ATMIA and the ASA is an evolving process, guidelines will be updated from time to time. Systems of good governance are essential for all organizations. However, they need to be implemented with unshakeable integrity and determination. Otherwise, they are just words on paper.

It is an honor for ATMIA to oversee the governance of the ATM Security Association at a time in the industry when there are cyber threats to ATM systems in addition to the on-going physical attacks and card and data compromise crimes. The merger of the two associations bodes well for the reinforcement of global defenses and deterrents to dent and blunt attacks against ATMs. There is much work to do together in the areas of best practices, crime data gathering and storage, education, collaboration with law enforcement and intelligence agencies, standards and security solutions. These operating policies and procedures will guide that work in a true spirit of transparency, dedication and, above all, integrity. We will build bold new systems of end-to-end protection to withstand the trickery and technology of the crooks.

Here's to a better era of strong, enhanced security for the world's estate of over three million ATMs. It can be done and it will be done.

Mike Lee

CEO, ATMIA

May 2019

Chapter 1. Mission

The mission of the ASA Operating Policies and Procedures is to govern the activities of the ATM Security Association and its working groups in a transparent, procompetitive way to strategically coordinate industry intelligence for understanding the emerging global threat landscape and for designing responses to ongoing criminal activity targeting the worldwide industry.

Chapter 2. Structure

The structure of the ATM Security Association positions the Joint Security Council as the ASA's governing body. It oversees the ATM Security Discussion Forum, a general forum for sharing and discussing current global attack trends and for recommending countermeasures.

In addition, the Joint Security Council oversees four working groups:

1. The ATM Cyber, Software and Encryption Security Alliance
2. The Next Gen ATM Security Committee
3. The Cassette Security Working Group
4. The ATM Skimming & Card Data Compromise Committee

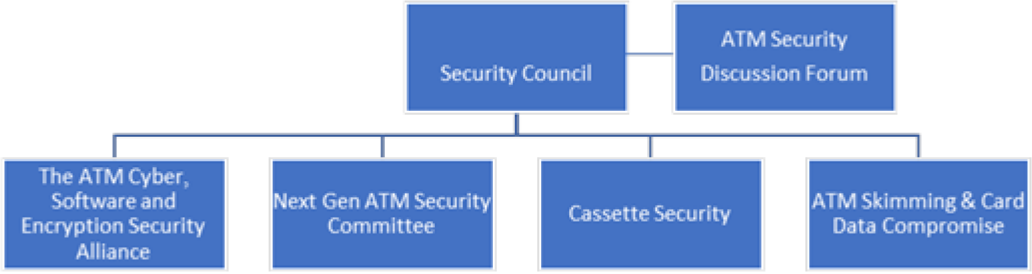
Security Council
ATM Security Discussion Forum
The ATM Cyber, Software and Encryption Security Alliance
Next Gen ATM Security Committee
Cassette Security
ATM Skimming & Card Data Compromise

Figure 1: The Structure of the ATM Security Association

Chapter 3. Working Groups and Task Forces

Working groups will be set up at the request of the members with the approval of the Joint Security Council.

A working group will function as a discussion and problem-solving body governed by the Joint Security Council. The focus of a working group typically covers a broad subject area. Topics and deliverables may evolve over the lifespan of that working group in the respective subject area.

The ATM Security Discussion Forum has been established to foster high-level information exchange between the members across all ASA groups. Information will include, but not be limited to, members' knowledge on global attack trends and security challenges, case studies and success stories.

The ATM Skimming & Card Data Compromise Working Group will function as a discussion and problem-solving working group focused on monitoring fraud trends and preventing ATM skimming, as well as other forms of card and card data compromise.

The Cassette Security Working Group will look at how to improve the security of ATM cassettes, including solutions and potential standards.

The ATM Cyber, Software and Encryption Security Alliance is a discussion and problem-solving working group focused on encryption and ways of protecting the ATM's cyber and software systems.

The Next Gen ATM Security Committee will oversee the security of the API App model for ATMs that will connect the ATM to the consumer's mobile phone for transactions. This working group will cover the security of consumer-owned devices and protecting the Next Gen ATM architecture.

Task forces will be set up at the request of the members with the approval of the Joint Security Council.

A task force will function as a targeted problem-solving body governed by the Joint Security Council. The action plan of a task force will focus on a designated topic and a defined deliverable.

Chapter 4. Operation of Working Groups and Task Forces

4.1. Chair of a Working Group

Every working group must have a Chair. The Chair of a working group may have backup assistants. In cases where the Chair is unable to execute his/her function, a nominated Deputy of the working group can assume the Chair's rights and responsibilities.

The Chair of a working group:

- Represents and manages the work of the working group;
- Calls and chairs the meetings of the working group;
- Creates and sends meeting agendas;
- Records and distributes meeting minutes; and
- Steers the operations of the working group and its attendees in accordance with relevant bylaws and operational policies and procedures.

4.2. Access to Working Groups

Any member can become part of a working group. It is the decision of the working group to accept new attendees in accordance with the Joint Security Council. The number of attendees in a working group is not limited. Attendees of a working group can be invited to or expelled from the working group by the Chair in accordance with the Joint Security Council.

4.3. Attendees of Working Groups

Attendees of working groups:

- Present initiatives and provide suggestions, opinions and proposals on issues within the scope of operations of the working group;
- Familiarize the working group with the position of the companies or institutions they represent;
- Ensure implementation of the joint conclusions;

- Conduct the duties within the competence of the working group in a responsible, legal and scrupulous manner; and
- Implement working group decisions.

Chapter 5. Meetings/Conference Calls

Scheduled meetings are held on a quarterly basis for the Joint Security Council and each of the working groups in Figure 1 on page 6. Extraordinary meetings may be convened as required to address specific issues.

5.1. Meetings will be run by the elected chairperson, or nominated deputy.

5.2. Agendas will be supplied at least two weeks prior.

5.3. Minutes will be distributed within 48 hours of each meeting.

5.4. Minutes need to be approved at the next meeting.

Chapter 6. Members and Subscribers

Paid-up members of ATMIA are permitted to participate in the working groups described in Chapter 2. Such participation is considered a member benefit.

In addition to this participation, members have the option to become annual subscribers.

6.1. Access to Benefits

Subscriber-only benefits include access to the following:

- Theoretical Risk Register
- Quarterly Global Crime Trends Analysis
- Research reports (Executive Summary to members; full report to subscribers)
- Security Best Practices (Executive Summary to members; full report to subscribers)
- Crime data
- Annual fraud survey (Executive Summary to members; full report to subscribers)

Subscriber-only benefits also include voting rights on proposals for standards and security solutions endorsements.

Both subscribers and members have access to the following:

- Research reports (Executive Summary to members; full report to subscribers)
- Security Best Practices (Executive Summary to members; full report to subscribers)
- Annual fraud survey (Executive Summary to members; full report to subscribers)

White papers are available to all members.

Press releases are available to the industry (without restrictions).

6.2. Categories of Subscribers

There are four categories of subscriber, depending on the sector and size of the company:

• Small Business*:	$250 p.a.
• Financial Institutions & Independent Deployers:	$500 p.a.
• ATM Suppliers/Service Providers:	$2,500 p.a.
• ATM Manufacturers:	$5,000 p.a.

*A small business is defined as having fewer than 10 employees.

Chapter 7. Voting

Voting may be by voice vote or by ballot. No single vote shall be split into fractional votes. Cumulative voting shall not be permitted.

A resolution shall only be passed if a vote is taken at a meeting of the members and the resolution is supported by a majority or super majority of the members entitled to vote (see following sections, 7.1 and 7.2).

7.1. Super Majority Votes

A super majority vote of the members shall be required for the following matters, which shall be an affirmative vote by at least two thirds (2/3) of the voting members present or represented at the meeting:

(a) Amendment of the bylaws

(b) Dissolution of the Association

7.2. Majority Votes

An affirmative vote of the members shall be required for the following matters, which shall be an affirmative vote by at least fifty-one percent (51%) of the voting members present or represented at the meeting:

(a) Any standards or standardization of products, processes or recommendations to be published by and in the name of the Association (for example, any standard response, design or implementation recommended with respect to a particular security threat)

(b) Decisions on topics and matters applicable to the working groups described under Structure in Chapter 2

7.3. Security Council Matters and Votes

The following matters shall be governed by the Joint Security Council:

(a) Approving and adopting the annual budget for the Association

(b) Approving the financial statements of the Association

(c) Adopting new trademarks or logos for the Association

(d) Establishing internal regulations to settle all questions for which no special provisions are made in the bylaws

(e) Approving the creation of, and charters for, any committee, or dissolving a committee

(f) Approving the creation of, and charters for, any working group, or dissolving a working group

(g) Amending or terminating any Association policies, including without limitation, Materials Policy, Intellectual Property Policy, Competition Policy, Trademark Policy, Board Committee Policy or Working Group Policy

(h) Expelling or suspending any member/subscriber

(i) Establishing and amending the membership fees, including the fee payment schedule and any proration of fees

(j) Appointing officers of the Association as provided in the bylaws

(k) Establishing compensation for officers of the Association (if applicable)

(l) Creating a branch or subsidiary

(m) Evaluating and procuring insurance (if any) to cover the Association and its activities

(n) Annual settlement of account

(o) Press releases

Chapter 8. Administrative Matters

8.1. Bookkeeping

Bookkeeping is subject to ATMIA's bylaws and operational policies and procedures.

8.2. Bank Account

The bank account is subject to ATMIA's banking procedures and budgeting processes.

8.3. Legal Services

Legal services are subject to ATMIA's legal counsel and bylaws.

8.4. Document Archive

All financial documents, including financial statements and balance sheets, will be stored electronically by ATMIA.

All agendas, minutes and letters will be stored electronically by ATMIA.

Chapter 9. Website and Secure Portal

9.1. Governance

The website falls under the governance of the Joint Security Council and ATMIA's IT management.

The website is subject to ATMIA's policy outlined in the Association's Policies and Procedures manual.

9.2. Publication of Material

Informational material is published at the sole discretion of the Association following the release by the Joint Security Council.

9.3. Secure Portal

Online access to the password-protected secure portal is for paid-up subscribers only, as defined in 6.1 Access to Benefits.

Chapter 10. Privacy Policies

The ASA adheres to the ATMIA Privacy Policy (https://www.atmia.com/privacy-policy/) and Terms of Use (https://www.atmia.com/terms-of-use/), which include GDPR (The General Data Protection Regulation 2016/679) requirements.