



# **ATM INTEGRITY TASK FORCE**

## **RECOMMENDATIONS ON BEST PRACTICES**

### **Report #1**

**Issue 1: Recommendations to Manufacturers for Improving PIN Security within the ATM**

**Issue 2: Best practices for ATM Acquiring entities – Sponsor FIs, ISOs and other ATM deployers, and other Service Providers**

**May 30, 2003**

**Electronic Funds Transfer Association**  
950 Herndon Parkway  
Herndon, VA 20170

## TABLE OF CONTENTS

<b>FOREWORD .....</b>	<b>1</b>
<b>INTRODUCTION .....</b>	<b>3</b>
Background – Task Force Formation .....	3
Task Force Objectives .....	4
Future Steps .....	5
Other Resource Materials .....	5
<b>Issue 1: RECOMMENDATIONS TO MANUFACTURERS FOR IMPROVING PIN SECURITY WITHIN THE ATM .....</b>	<b>6</b>
<b>Issue 2: BEST PRACTICES FOR ATM ACQUIRING ENTITIES – SPONSOR FIs, ISOs AND OTHER ATM DEPLOYERS, AND OTHER SERVICE PROVIDERS .....</b>	<b>8</b>
1. Applicability .....	8
2. Due Diligence .....	8
3. Training .....	10
4. On-going obligations .....	11
<b>ACKNOWLEDGEMENTS .....</b>	<b>12</b>

## FOREWORD

We are entering a period in time where we must renew emphasis on the security of the ATM services infrastructure both in the US and globally. The confluence of industry growth, technology evolution, the increasing sophistication of criminal attacks, and the new geopolitical landscape and realities after September 11, 2001 makes such action not a luxury of choice but a necessary mandate.

Modern ATM services are based on a complex operating infrastructure involving many specialized entities in the overall financial services market whose needs, capabilities, and economics must be balanced to ensure that these services operate in the secure, efficient and cost-effective manner which consumers and all market participants have come to expect. Any initiatives for change need the participation and acceptance of all segments of the industry.

The Electronic Funds Transfer Association (EFTA) decided to undertake such an initiative to bring about consensus on security enhancements to the industry-wide ATM services infrastructure. EFTA is a unique multi-industry forum with a focus on electronics payments services and with membership drawn from all segments of the Electronic Funds Transfer Industry. As such it is ideally positioned to facilitate such an industry-wide effort.

EFTA established an ATM Security Task Force and charged it with developing recommendations on Best Practices which would be responsive to the short and long term issues exposed in recent attacks on the ATM installed base.

This report is the first generated by the Task Force and contains its recommendations on Best Practices in two areas:

1. Recommendations to Manufacturers for Improving PIN Security within the ATM
2. Best practices for ATM Acquiring entities – Sponsor FI, ISOs and other ATM deployers, and other Service Providers

This report should be read keeping in mind several critical elements of context.

- ❖ These Recommendations on Best Practices are narrowly focused on manufacturer and acquiring entity actions. The focus of this report is a result of prioritizing on the critical points of weaknesses uncovered in the attacks which were the impetus to the formation of the Task Force. *This focus is not meant to imply that these are the only entities which impact or are impacted by ATM security issues.*
- ❖ The EFTA Task Force and Board recognize that the effective management of the service delivery process of electronic fund transfer involves comprehensive "Best Practices" on the part of all entities in the services cycle. Subsequent reports may address

suggestions for other segments of the industry such as Issuers, Networks, and Processors.

- ❖ *These Recommendations on Best Practices are not to be construed as mandatory requirements for any entity in the ATM industry, whether or not such entity is a member of EFTA. Many of these recommendations are already established business practices for business entities within the affected segments of the market. However, each affected entity will need to review and, if necessary, establish its own processes to meet its own needs and to ensure it complies with any Operating Rules of the Networks in which it participates.*
- ❖ *Nothing in these Recommendations on Best Practices should be construed to guarantee adherence to these Best Practices by any EFTA member or non-member entity, either as a continuation of current practice or through adoption in the future.*
- ❖ *It is also important to recognize that even complete adherence to these Recommendations on Best Practices by manufacturers and acquiring entities cannot completely eliminate all the risks inherent in the delivery of ATM services. (A recent attack has highlighted this by capturing card data through compromise of the card reader not at the ATM itself but at the controlling entrance to the ATM vestibule. This, in conjunction with a wireless video camera to capture PINS, provided the information necessary to compromise ATM cards.)*

The EFTA Board hopes that this Report makes a contribution to the ATM industry's ongoing efforts to continuously enhance the integrity of its service delivery. The EFTA Board also sincerely appreciates the commitment of all who made this report possible; more detailed acknowledgements are provided in a separate section at the end of this report.

## INTRODUCTION

### ***Background – Task Force Formation***

The ATM industry has grown and changed substantially over the last decade. US consumers carry about 254 million ATM cards and are able to use them at about 315,000 ATMs installed in the USA, almost four times as many as at the start of the decade. Whereas at the beginning of the industry, the majority of the ATMs were Financial Institution (FI) owned and deployed on their premises, today about 60% of the machines are located off-FI-premises, and about 35% of the installed base is owned or controlled by approximately 300 Independent Sales Organizations (ISOs).

Connectivity in the US is almost universal. Consumers expect to be able to use their card at any ATM they see, and they are rarely disappointed. The international card associations are developing significant presence at the approximately 1.1 million ATMs installed worldwide, thus further extending this connectivity to a global scale.

While this growth of ATM services has presented consumers with highly valued convenience, it has also presented criminals with an increasingly attractive target for fraudulent attack. The fundamental security mechanisms for ATM services have remained largely unchanged over the last thirty years. In the early years of the industry, the techniques used in attacks at the ATM itself rarely compromised large numbers of cards. Today, criminal attacks on FI-issued payments cards at both ATMs and points-of-sale (POS) are becoming increasingly sophisticated in terms of scale, technology employed, funding and planning and execution.

The present concern is not over traditional fraud that compromises a small number of cards, but over larger attacks which can compromise cards in the thousands with resulting high fraud losses in the millions. The total “hard dollar” costs of such attacks is significantly larger when all of the ancillary operations costs to recover from such attacks is taken into account; a study by HNC Card Alert Services in 1995 estimated total costs at four times the direct fraud losses involved. The adverse impacts in loss of consumer confidence and negative publicity are harder to quantify but are real nevertheless.

These traditional concerns over loss prevention for consumers and industry participation have since taken on a dimension of national and international security. The US Treasury has concerns about the various ways in which terrorists might use the ATM infrastructure -- as a funds distribution channel, as a source of funds through fraudulent schemes, as a vehicle to launder money, or even possibly to creating chaos in economies through attacks on public confidence in the integrity of payment systems.

Unfortunately, these concerns are far from theoretical. A recent successful card skimming attack unleashed in New York in mid-2001 through 2002 involved the use of over twenty altered ATMs to compromise thousands of cards at hundreds of FIs. The aggregated losses at just thirty five FIs totaled over \$3.5 million. This case was

intensively investigated by the US Secret Service and was eventually cracked by the cooperation of many segments of the ATM industry.

The challenges in the investigation of this recent attack highlighted the growth in complexity of the structure of the industry. Today, participation in the industry goes well beyond FIs and ATM manufacturers to include shared networks, processors, and a wide range of specialist service providers such as ISOs, Encryption Service Organizations (ESOs), cash servicers, and maintenance organizations, along with merchants and other entities that control the locations at which the ATMs are deployed.

During the course of their investigations, the US Secret Service recognized the high benefit in industry-wide collaboration to improve the integrity of ATM transactions and services. As one part of their efforts to stimulate such collaboration they approached the Electronic Funds Transfer Association (EFTA).

EFTA is a unique multi-industry forum with membership drawn from all segments of the Electronic Funds Transfer Industry. As such it is ideally positioned to facilitate such an industry-wide effort. Discussions between the US Secret Service, EFTA Board Member Mike Hudson and Executive Director Kurt Helwig provided the background for an EFTA Board discussion of this topic. Subsequently, the EFTA Board of Directors authorized the formation of The ATM Integrity Task Force with Mike Hudson, EVP of Tidel Engineering, as its volunteer Chair. A number of EFTA member organizations agreed to actively participate.

### ***Task Force Objectives***

Early in its deliberations the Task Force recognized that the overall security of the ATM infrastructure was a wide subject and had overlaps with other payments services including point-of-sale where the same card is used, and transactions often flow over the same infrastructure. The Task Force agreed to focus initially on attacks targeted at large scale card and PIN data capture at the ATM.

The rationale for this focus was that this problem is very real; it is immediate; it is significant and non-trivial in its impacts; it has no solution accepted across the industry; it is law enforcement's priority and where it is seeking immediate help; it is a Financial Industry priority; it is in emerging regulatory cross-hairs; and it is the initial impetus for the formation of the Task Force in the first place.

This led to a Task Force to initially address two issues, which between them cover the major exposures which were exploited in the recent attacks on the installed base:

1. Recommendations to Manufacturers for Improving PIN Security within the ATM
2. Best practices for ATM Acquiring entities – Sponsor FIs, ISOs and other ATM deployers, and other Service Providers

It was also agreed that the broader issues could be tackled under the aegis of an EFTA Council which could identify, prioritize and assign other issues to future Task Forces geared specifically to address them.

### ***Future Steps***

In the future, EFTA expects to consider, prioritize and address additional issues such as:

- ❖ Recommendations on Best Practices for other entities in the ATM service delivery chain.
- ❖ Protection of ATMs against external physical attack or alteration.
- ❖ Information sharing at all levels, across organizations and with Government agencies subject to all relevant laws including The Privacy and Patriot Acts.
- ❖ Aggregation and publication of statistics and status of major fraud schemes.
- ❖ Coordination with international investigative bodies.
- ❖ Potentially, the long term evolution of service infrastructure to next generation card technology including:
  - Short, mid and long term technology and implementation strategy.
  - Business cases.
  - Migration processes.

### ***Other Resource Materials***

Task Force members submitted other related materials to support the deliberations of the Task Force. EFTA members may view these materials on the EFTA website at [www.EFTA.org](http://www.EFTA.org).

## **Issue 1: RECOMMENDATIONS TO MANUFACTURERS FOR IMPROVING PIN SECURITY WITHIN THE ATM**

The EFTA ATM Integrity Task Force recommends that manufacturers adopt the following practices to improve PIN Security within the ATM.

1. The existing standards for key management and PIN security should remain the standard to which ATMs should adhere with respect to encryption and key management. In the U.S., these standards are the ANSI X9.24 for Key Management and ANSI X9.8 for PIN encryption. ISO has established standards which have global acceptance, and local standards will also have to be adhered to such as GIE CB for France, and ZKA for Germany.
2. In the past, the key management and encryption requirements of ANSI X9.24 and ANSI X9.8 have been subject to different interpretations. As a result, many of the “legacy” (existing) ATMs deployed in the U.S., while self-certified by manufacturers as meeting those standards, may not meet the standards as interpreted by the PIN-Debit Networks.
3. Manufacturers use different nomenclature to describe the current generation of ATM PIN Pads where the PIN security boundary begins at the surface of the PIN Pad and encompasses all interfaces through and into the security module. Terms include Tamper Resistant Encrypting PIN Pad (TREPP), Encrypting PIN Pad (EPP), SPED, etc. This recommendation is intended to apply to the device regardless of the manufacturer's nomenclature.
4. All of the major manufacturers (including but not limited to Diebold, Fujitsu, NCR, Nextran, Tidel, Tranax, Triton, and Wincor-Nixdorf) should form a representative group of manufacturers to:

- a. Develop a common interpretation of these standards.

One element of this interpretation should be that the use of a proprietary encryption methodology to protect the PIN between the key contact and the security module is not consistent with the intent of the standard. All ATMs should follow the industry encryption standards from the point of initial PIN entry and through the entire system.

- b. Ensure this interpretation is consistent with network intent and interpretations.
- c. Collectively present a request to Underwriters Laboratory ("UL") and other independent testing authorities to modify the existing UL291 standard for ATMs so as to include a certification that the UL approved model meets the standards as interpreted.

Future UL291 listings would, therefore, include interpretation of the standards, and all manufacturers seeking such listings would be evaluated against this common standard by an independent third party.

Similar action with other certifying bodies such as CE could also be implemented.

5. Taking into consideration recent rules changes put into effect by Visa, and certification requirements stated by major Networks, manufacturers should communicate that all current and future equipment manufactured by them meets the ANSI X9.8 and ANSI X9.24 standards (and other international standards applicable in each country) as clarified with respect to:
  - a. The point at which the PIN is entered into the system (i.e., the external surface of the keyboard);
  - b. The point at which the PIN is encrypted for transmission;
  - c. The path between the above-noted two (2) points.

It should be noted that current production models of many, if not all, major manufacturers are believed to have encrypting PIN Pads consistent with this recommended interpretation.

6. Manufacturers, if they have not already done so, should identify:
  - a. Legacy machines, by model description, that will be able to be upgraded to the above-defined standards;
  - b. The upgrade path (i.e., replacement kits, software upgrades, etc.) available for these upgradeable legacy machines;
  - c. Those legacy machines that do not and will not have upgrade paths available to them.
7. The schedule for compliance of legacy machines that can be upgraded through use of upgrades/retrofit kits should enable these upgrades to occur in conjunction with other previously established timetables for upgrades to comply with DES 3 and other mandates, so as to maximize efficiency and minimize costs associated with such upgrades of the installed ATM base.

## **Issue 2: BEST PRACTICES FOR ATM ACQUIRING ENTITIES – SPONSOR FIs, ISOs AND OTHER ATM DEPLOYERS, AND OTHER SERVICE PROVIDERS**

### **1. *Applicability***

ATM operations depend on a chain of parties, from the Networks, to the Sponsor Financial Institutions (SFI), to the Independent Sales Organizations (ISO), and to the service providers. ISOs may employ services from a variety of organizations including, but not limited to, processors, Encryption Service Organizations (ESO), ATM service and maintenance providers, and cash replenishers (i.e., armored carriers). Parties sponsored by SFIs and service providers include ISOs, processors, ESOs, ATM maintenance organizations, and cash services.

There are also institutions that do not sponsor other entities into the Networks but deploy ATMs as Acquirers. Many of these deployers use third parties to perform maintenance and cash replenishment services for both off-premises and on-premises ATMs.

Implementing the recommended Best Practices is viewed as a means by which all participants throughout the ATM chain can help protect the integrity of the EFT transaction.

### **2. *Due Diligence***

ATM Acquirers and SFIs should consider the following examinations and criteria as part of any due diligence of any third party they wish to sponsor. SFIs should strongly recommend similar due diligence be employed by their sponsored ISOs for any employed service provider that they utilize.

- a) A comprehensive financial review, including a review of current audited financial statements, when available. Appropriate additional investigations (i.e., D & B credit check) should be exercised if audited statements are not available.
- b) A review of the responsible parties (i.e., corporation, partnership, principle owner or executive officer), business tax returns, statements of net worth and liabilities, and proof of ability to support any liabilities to be incurred.
- c) Validate identification of the principals and of the key agents used by the sponsored or employed entity. Validation may be personal verification or professional investigation of such items as:
  - c.1 Name – Social Security Number match;
  - c.2 Criminal records;
  - c.3 Residency – Citizenship, legal residency, or legal alien status;
  - c.4 Check against the OFAC list (Office of Foreign Assets Control);
  - c.5 Business records as available from the Lexis – Nexis or similar databases;
  - c.6 Other such items as may be required.

*Credit and other investigations should be conducted in accordance with applicable law, including appropriate use of credit reporting agencies, and appropriate notice to the party being investigated to the extent required.*

- d) A review of all current and previous Acquirer business relationships, both foreign and domestic, including all DBAs used by the ISO and its principals.

*At present, such information is not easily attainable without the cooperation of the ISO itself. The preferred solution would be to develop industry practices pursuant to which a potential SFI can get relevant information from Networks or previous SFIs in accordance with any applicable legal constraints. Such information would indicate whether any prior relationships had been terminated for "cause" or simply for commercial reasons, without disclosing the details, particularly of the latter.*

- e) Ensure that comprehensive and verifiable terminal inventory procedures and controls are established and implemented which identify the location of all terminals including those in the installed base, whether initially installed at a location or subsequently relocated.
- f) An audit conducted by the SFI, a qualified independent entity or a self-audit, of the ISOs procedures for PIN, data security and privacy to verify that they meet the Network's standards. Where the audit is not conducted by the SFI, it is the SFI's responsibility to review the audit and to decide whether or not to accept it in lieu of conducting its own audit.
- g) SFIs should be aware of the use of other sub-contractors to perform services for which it contracts with an ISO.
- g.1 Sub-contractors should be registered with the SFI and with the Networks in which the SFI participates, if such registration is required by the Network Operating Rules.
- h) A review of the soundness of the general business and operating practices of the ISO with respect to its ability to manage the risks inherent in its business. Examples of such processes include:
- Knowledge of the parties with which it contracts ("know their customer");
  - Adequate operating reporting processes;
  - Adequate record keeping – contracts, addresses, protection of records, etc.;
  - Adequate exception reporting processes.
- i) Because there is no clear certification standard today, SFIs should ensure that manufacturers have certified that the ATMs employed comply with the Network security standards, including those for encrypted PIN pads, which are developed as a result of the actions recommended for manufacturers (Issue 1, Paragraphs 4 and 5). However, in no event should an SFI accept for sponsorship any device that has been ruled non-compliant by the Network, regardless of claims by its manufacturer.

- j) The SFIs due diligence review, signed by a senior officer of the SFI, should stress reliance on the SFI's due diligence process, and not solely upon language in the Agreement with the ISO which passes through Sponsor's liability to that ISO.
- k) Due diligence records should be maintained at the SFI, and be available on request to the Network and to appropriately authorized law enforcement agencies through the duration of the contract and for a reasonable period thereafter or as defined by Network Rules.

### **3. Training**

Networks should provide SFI and its ISOs Network-approved training sessions on Network Rules and Standards.

- a) SFIs may attend training with any ISO they sponsor, and it is recommended they take the opportunity to attend these sessions to train new personnel or to update existing personnel.
- b) Networks should require ISOs to attend the training session as they are first signed up.
- c) In addition to individual Network Rules, the basic content of such courses might include:
  - Terminology and Definitions
  - Technology and Operations Overview
  - System Integrity and Security
    - Terminal requirements
    - PIN encryption and management processes
    - Data privacy requirements
    - Other operational requirements
  - Fraud – financial exposure and practices
    - Liability under Network Rules
  - Registration Process

*It would be ideal to have cross-acceptance of training across Networks under which training courses would be certified as covering some basic material. A third party passing one of these courses would not have to go through it again for admission to another Network. It was noted that the major roadblock to developing a common certification is that aside from such general material, training usually also includes Network specific Rules which differ across Networks.*

#### **4. On-going obligations**

All Networks presently require that SFIs meet their settlement obligations, ensure compliance with the Network Rules and Standards by their Sponsored Parties, and be fully liable for the actions of all of their sponsored parties and sponsored entities. In addition:

- a) The SFI should monitor the operations of its sponsored parties and of its own sponsorship business on an on-going basis. The SFI should:
  - a.1 Require and review reports of ATM deployment locations and redeployments. (Pursuant to recently published PLUS Operating Rule requirements.)
  - a.2 Require and review standard reports on operations.
  - a.3 Perform random checks or audits of reports to ensure operations are in compliance with Network Rules and Standards.
- b) Maintain current records reflecting any changes to the sponsored parties including, but not limited to:
  - b.1 Change of ownership;
  - b.2 Name or address change of ISO;
  - b.3 Assumption of a new DBA by ISO;
  - b.4 Report to the Network, within a reasonable time, termination of its relationship with an ISO.

## ACKNOWLEDGEMENTS

The EFTA Board would like to extend its appreciation to all of the individuals on the ATM Integrity Task Force, and the organizations they represent, for their participation and support without which these Best Practices could not have been drafted. Not all members were able to attend each of the four meetings held by the Task Force but everyone contributed valuable input over the process as a whole.

While it is impossible to acknowledge the efforts of all members individually, the Board would like to recognize the additional efforts of some individuals and organizations.

US Secret Service Agent Gregg James, who plays a major role in the investigation of the recent ATM attacks and ATM fraud in general, was instrumental in urging EFTA to utilize its cross-industry membership to attack this industry-wide problem and provided several important briefings to the Task Force on the status of the investigations and on the key issues which had to be resolved.

Mark Dimodica, eFunds assisted by Sandra Hartfield, Palm Desert National Bank; Doug Sholes, Triton Systems; and Michael Urban, Fair Isaac and Company, developed a working paper to help assess risks during the service life cycle for ATM services. While this was not finalized as part of the current initiative it provided a starting point for further discussions.

The Recommendations to Manufacturers for Improving PIN Security within the ATM were initially developed by a panel headed by Mike Hudson, Tidel Engineering and Chairman of the Task Force ([mhudson@tidel.com](mailto:mhudson@tidel.com)). Panel members included:

Rick Duvall	ACI Worldwide	<a href="mailto:duvallr@aciworldwide.com">duvallr@aciworldwide.com</a>
Lyle Elias	ATMIA	<a href="mailto:lyle.elias@valuepaymentnetwork.com">lyle.elias@valuepaymentnetwork.com</a>
Patrick Tolman	Bank of America	<a href="mailto:patrick.a.tolman@bankofamerica.com">patrick.a.tolman@bankofamerica.com</a>
Anna Istnick	Diebold	<a href="mailto:Istnica@diebold.com">Istnica@diebold.com</a>
Mike Urban	Fair, Isaac, and Company	<a href="mailto:mike.urban@fairisaaac.com">mike.urban@fairisaaac.com</a>
Eric Park	Innobeta Systems	<a href="mailto:eric@innobeta.com">eric@innobeta.com</a>
Alan Russell	NCR	<a href="mailto:alan.russell@ncr.com">alan.russell@ncr.com</a>
Beth Lynn	Star System, Inc.	<a href="mailto:blynn@star-system.com">blynn@star-system.com</a>
Cindy Provin	Thales e-Security	<a href="mailto:cindy.provin@thales-ecurity.com">cindy.provin@thales-ecurity.com</a>
Flynt Moreland	Tidel Engineering	<a href="mailto:flynt@tidel.com">flynt@tidel.com</a>
Mindy DeTorres	Visa International	<a href="mailto:mdetorres@visa.com">mdetorres@visa.com</a>

The Best Practices for ATM Acquiring entities – Acquirer FIs, Sponsor FIs, ISOs and other ATM deployers, and other Service Providers – were initially developed by a panel headed by Noshir Kathok, Noshir Group Inc. ([noshir@noshirgroup.com](mailto:noshir@noshirgroup.com)). Noshir Kathok also prepared the initial draft. Panel members included:

Ellen Stebbins	ATMIA	<a href="mailto:ellens@first-american.net">ellens@first-american.net</a>
Doug Deitel	Cardtronics	<a href="mailto:ddeitel@cardtronics.com">ddeitel@cardtronics.com</a>
Harry Houck	Citibank	<a href="mailto:Harry.j.houck@citicorp.com">Harry.j.houck@citicorp.com</a>
Michael LoPresti	Citibank	<a href="mailto:Michael.lopresti@citicorp.com">Michael.lopresti@citicorp.com</a>
Dennis Ambach	eFunds Corp.	<a href="mailto:Dennis_ambach@efunds.com">Dennis_ambach@efunds.com</a>
Kathy Sutton	ICBA Bancard	<a href="mailto:Kathy.sutton@icba.org">Kathy.sutton@icba.org</a>
Martyn Gould	LINK	<a href="mailto:mgould@link.co.uk">mgould@link.co.uk</a>
John Schettino	MasterCard International	<a href="mailto:John_schettino@mastercard.com">John_schettino@mastercard.com</a>
Douglas Baun	Metavante Corp.	<a href="mailto:Doug.baum@metavante.com">Doug.baum@metavante.com</a>
Susan Zawodniak.	NYCE Corp	<a href="mailto:Susan_zawodniak@nyce.net">Susan_zawodniak@nyce.net</a>
Sandra Hartfield	Palm Desert National Bank	<a href="mailto:shartfield@pdnb.com">shartfield@pdnb.com</a>
Sharon Lappin	Star Systems Inc.	<a href="mailto:slappin@neteps.com">slappin@neteps.com</a>
Gregg James	USSS	<a href="mailto:gjames@uss.s.treas.gov">gjames@uss.s.treas.gov</a>
Norman Litell	Visa USA	<a href="mailto:nlitell@visa.com">nlitell@visa.com</a>

The initial drafts were created as a result of Task Force deliberations at its third meeting. The drafts were subsequently reviewed by participants at the fourth meeting. This meeting did not include all of the members present for the original discussions, but did include some new attendees.

Lana Harmelink of the ATMIA Board reviewed the drafts and provided the Association’s input. Sandra Hartfield and Mike Hudson provided additional detailed reviews.

Kiran Gandhi, MagTek and John Schettino, MasterCard provided a presentation and live demonstration of a card protection technology, Magneprint, at short notice. Norman Litell, Visa, provided background materials and briefings on recent related actions taken by Visa and other market entities. EFTA members may view these and other related materials on the EFTA website at [www.EFTA.org](http://www.EFTA.org).

Mike Hudson took on the challenge of directing the Task Force as its Chairman. Noshir Kathok, Noshir Group, Inc. acted as facilitator, generated the meeting reports, and



developed this final report. Melanie Renner of EFTA performed the thankless but essential task of arranging and coordinating the meetings.