Alliance for Financial Inclusion
Bringing smart policies to life

Mobile Financial Services Working Group (MFSWG)

# Mobile Financial Services Technology Risks

This guideline note was developed by AFI's Mobile Financial Services Working Group (MFSWG) to identify the types of technology risks inherent in mobile financial services and strategies to manage them.

Guideline Note No.2
March 2013

# Contents

Recognizing the potential of mobile financial services (MFS), the Mobile Financial Services Working Group (MFSWG) was created to provide a platform within the AFI network for policymaker discussion on regulatory issues related to MFS. The working group promotes the broad use of MFS as a key solution for greater financial inclusion in emerging and developing countries. The group aims to stimulate discussion and learning among policymakers and promote greater coordination between the many different MFS actors, such as financial and telecommunications regulators and bank and non-bank providers.

## Context

Mobile financial services (MFS) offer the possibility of greater efficiency and convenience in payments applications and could also provide a foundation for financial inclusion initiatives. For MFS to deliver on their promise, however, service providers and regulators must seriously consider platform security within this new market.

Because business models, market needs, and regulatory forbearance will vary from country to country, this note does not set out a single set of policies appropriate to all contexts. Instead, it is intended to help orient policymaking by identifying the types of technology risks that are endemic to mobile financial services and the strategies for managing them. This note therefore charts the flow of information in MFS transactions, identifies the types of technology risks that apply to these information flows, and articulates frameworks for risk management and monitoring. The goal of this note is to help regulators to start thinking about technology risks in MFS in a flexible way that will be useful for future decision-making.

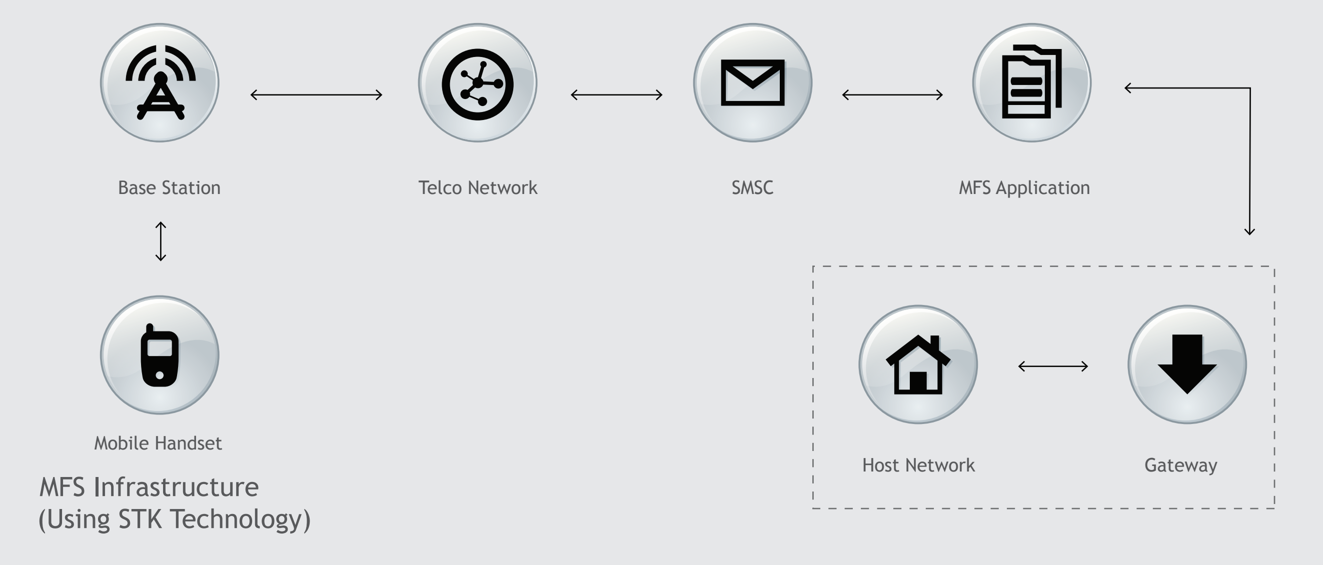
**A note on language:** Throughout this note, the term ***"threats"*** is used to describe the classes of dysfunction in a MFS service offering and ***"risks"*** refers to the application of those threats to the actual processes implied in a MFS offering. In this sense, risks are instances of threats that are observable in real-world transactions.

## Information flows in MFS

Regulators need to familiarize themselves with how information flows within the MFS network in order to analyze the technical risks that evolve in this environment. If you understand how each element in the network handles information, you can therefore identify the types of controls required to guarantee the security of this information. Figure 1 is a schematic representation of these information flows for a bank-based MFS service offered in partnership with a mobile network operator (MNO).

MFS users initiate processes using their handsets. The information provided by each user is then sent to the MNO's base station.[1] In a GSM network, the base station receives a channel request from the mobile handset and forwards it to the user's MNO. With SMS transactions, data packets containing transaction information are processed at a short messaging service center (SMSC) and routed to the MFS application server. In turn, the MFS application server delivers the transaction information to a gateway – the interface between the MNO's network and the bank's network. The data packet is then subjected to a security check and, pending clearance, is routed to the bank's internal network for authorization and further processing. The bank's network stores the user's financial and non-financial information and authorizes the transaction requested by the user. Because this process operates in reverse, it is at this point that the user is notified about the completed transaction.

Figure 1: The infrastructure of mobile financial services (using STK technology)



[1] Any message sent by the handset has an identification code which will then be used by the base station to determine whether the network used by the sender belongs to them. If it does, the message will be forwarded to the telco network. If not, the message will be dropped. The handset will then continue searching for a base station that will cater its request until a complete handshake has taken place.

## Classification of technology threats

It is important to understand the flow of information in MFS transactions because a variety of technology risks are present at each stage of this flow. Indeed, it is useful to organize technology risks according to their larger threat category. Dhillon (2007) identifies six general categories of threats in information systems:

**Modification:** when information in the system is accessed without authorization and changed without permission.

**Destruction:** when hardware, software, data or communications channels are destroyed or lost.

**Disclosure:** when data is made available without the owner's consent.

**Interception:** when an unauthorized person or software gains access to information resources, thereby allowing programs and other confidential information to be copied without authorization.

**Interruption:** when service or resources become unavailable for use, either accidentally or intentionally.

**Fabrication:** when false transactions are inserted into a record or added to a database by an unauthorized user.

This threat framework can be applied to the process diagram of information flows in MFS.

Figure 2 presents a non-exhaustive view of the points at which threats can be introduced in MFS information flows.

Table 1. Classification of MFS technology threats

| Threats | Data | Software | Hardware | Communications Channel |
|---|---|---|---|---|
| Modification | Occurs during storage, transmission, and change in physical hardware | Occurs when software is altered to perform additional functions or computations | -- | Occurs when packets are routed toward a different destination |
| Destruction | Caused by failure of hardware and/or software | Destruction due to malicious intent, i.e. malicious software (malware) | Caused by natural calamities such as floods, fire, or terrorist attacks | Caused by fiber optic or leased line cuts due to unexpected events, i.e. flooding, stealing, or road construction |
| Disclosure | Occurs when there is unauthorized access of another person's data/ information | -- | -- | -- |
| Interception | Occurs when confidential information is replicated by unauthorized users | Occurs when software programs are illegitimately copied from a computer resource | Occurs when unauthorized users gain physical access to hardware | Occurs when a third party was able to tap (listen to) ports without legitimate users' knowledge |
| Interruption | -- | • Caused by erasing software programs and/or specific functionalities<br>• Can be a result of operating system corruption | Caused by damaged hardware | • Caused by malicious attacks, such as flooding and denial-of-service<br>• Can be a result of natural calamities, power outage, problem with base stations, or network problems |
| Fabrication | Caused by phishing attacks | -- | -- | -- |

Reference: Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases.*

## Identifying MFS technology risks

The classificatory framework provided by the language of threats can help us make sense of the profusion of technology risks that afflict MFS. These risks are specific and varied, but placing them within an ontology of threats can help to organize, avoid, and eventually remedy them. This section highlights specific risks and organizes them according to the larger class of threats to which they belong.

### Threat: Modification

### Infection by mobile malware (risk)

Malware attacks are common in the PC environment and they are expected to spread to mobile devices suddenly and soon. Malware attacks in mobile phones can occur as follows:[2]

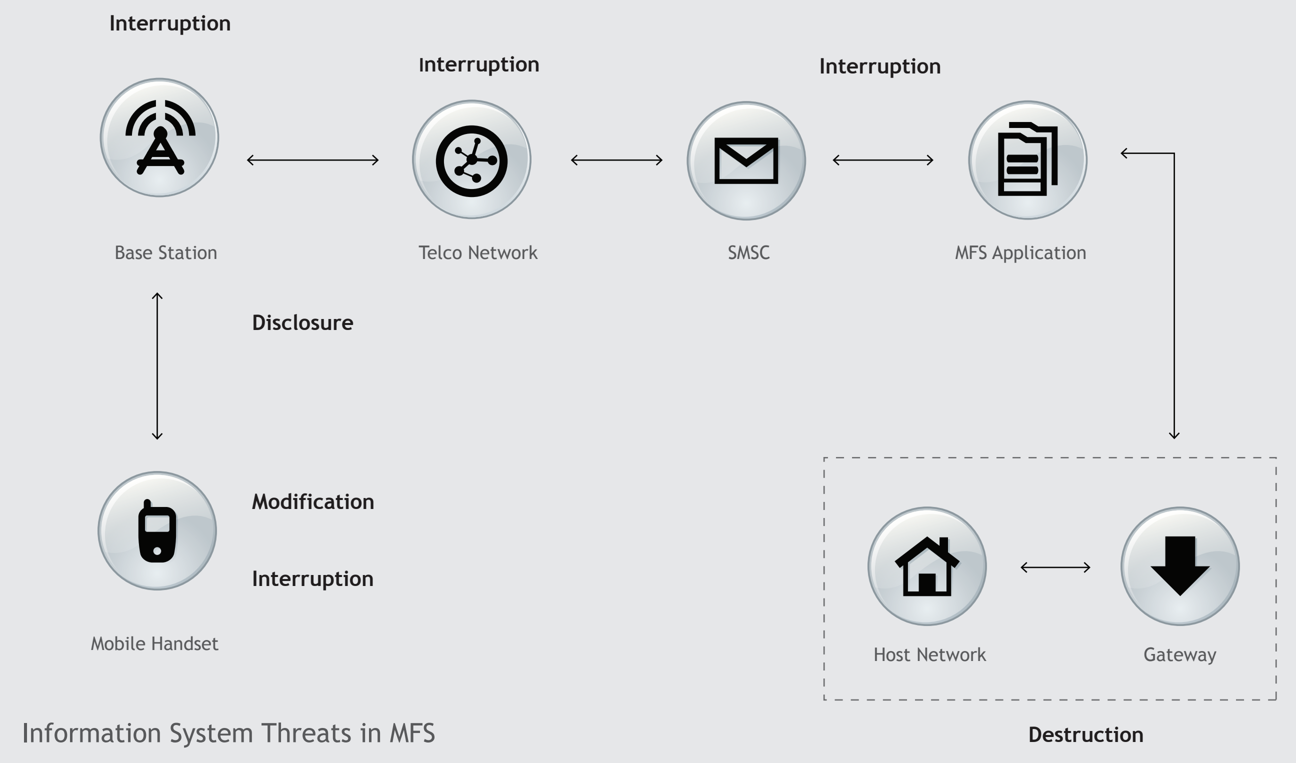
- Malware virus/trojans/worms can spread via Bluetooth and MMS.
- Malware can manipulate a user by sending a SMS message.
- Malicious software can infect files.
- Attackers can gain remote access of mobile phones by spreading malware.
- Malware, when downloaded, can change icons and system applications.
- Malware can install non-operational functions and applications.
- Malware is a useful channel that can be used to install other malicious programs.
- Malware can steal any data or information entered by the user and blocks the use of memory cards.

### Threat: Disclosure

### Readability of customers' critical financial information via SMS (risk)

Readability is a major concern when using SMS to access accounts and receive notifications about previous activities. SMS are transmitted and received in clear text and this protocol does not use any encryption techniques. In cases of device theft and malicious software, unauthorized users can gain full access to a customer's account.

Figure 2: Information system threats to MFS



[2] Gostev, A., 2006.

**Threat: Disclosure**

### Exposure of critical data due to insecure end-to-end encryption (risk)

Wireless Application Protocol (WAP) is an application standard that allows mobile handsets to access the internet. WAP-enabled mobile phones use browsers similar to those used by computers, although they have modifications to accommodate the restrictions of mobile phones. WAP uses the same layered approach as that of TCP-IP. A normal computer-based website allows users to access the internet by using the application layer protocol HTML. Likewise, consumers with WAP-enabled handsets can access the same website using their mobile phones by means of WML (Wireless Markup Language) protocol, which is an application layer of WAP. The only difference between the two is the size and resolution of the display (since the website is converted to cater to the restrictions of the handset). Unencrypted transmissions are therefore vulnerable to being exposed to unauthorized parties.

**Threat: Interruption**

### Unavailability of communication channel due to Denial-of-Service attacks (risk)

Denial-of-Service (DOS) attacks make a computer resource unavailable by flooding or consuming the component's resource. DOS attacks most commonly target servers and databases, which can also affect mobile networks because both the wired and wireless environment use the same infrastructure.

**Threat: Interception**

### Cross-scripting attack in USSD (risk)

The communication protocol USSD allows faster data transmission compared to SMS. Unlike SMS, USSD uses a direct connection between sender and recipient. It is a session-oriented communication channel, wherein the USSD application is used as an interface between the telecommunications provider and the customer's bank account. USSD can also be managed using web-based applications, so it is therefore prone to cross-site scripting attacks. In these attacks, a malicious user exploits the vulnerability of the web-based application installed in the user's handset to manipulate transactions (by injecting a Java or SQL script to steal the user's critical information). They can also perform malicious actions in the database, take over another user's active session, and connect users to malicious servers.

This list of risks is not intended to be exhaustive, but it illustrates the types of risks that any service offering needs to manage. With these risks in mind, we now turn to the principles of risk management and monitoring that regulators need to know.

Table 2. Risk Impact Model

| LIKELIHOOD | IMPACT | | | | |
|---|---|---|---|---|---|
| | Catastrophic | High | Moderate | Low | Insignificant |
| Almost certain | E | E | E | H | M |
| Likely | E | E | H | H | M |
| Possible | E | E | H | M | L |
| Unlikely | E | H | M | L | L |
| Rare | H | H | M | L | L |

LEVEL OF RISK: E=Extreme H=High M=Moderate L=Low

## MFS technology risks: Management and monitoring

### PRINCIPLES

There are five key principles guiding technology risk management in MFS: Confidentiality, Integrity, Availability, Authentication, and Non-repudiation. Each of these principles is examined below.

**Confidentiality:** to protect user data from unauthorized access or theft. It is important to distinguish between financial and non-financial data because different confidentiality principles apply to each. In general, financial data requires the strongest encryption standards in display, storage, and transmission. Personal identification numbers should be stored in encrypted form and be unavailable to service provider staff. Strong cryptography standards should be applied to data transmitted over public networks, such as the internet and cellular networks. Non-financial data can be kept confidential with slightly less stringent steps, such as establishing firewalls, implementing intrusion prevention and detection systems, and using access controls.

**Integrity:** the completeness, accuracy, and trustworthiness of data being presented. To validate data integrity, verify the process that identifies missing fields, performs sequence checks, and checks hash total[3] and variable length. Data integrity is most important during transmission because interception and data manipulation are most likely to happen at this stage.

**Availability:** that data and service should be accessible whenever legitimate users want to use MFS. There are a number of scenarios that can threaten data and service availability. Technical risks to service availability include environmental calamities (such as power outages, terrorist attacks, and acts of nature) and malicious action, such as denial-of-service attacks.

**Authentication:** establishing user and service provider identity.

- **Users** must be confident that the host requesting connection is authorized and that there are no third parties involved in the connection between the terminal and host servers. This also includes access control, permission control, and password authentication.
- **Service providers** must be confident that the person accessing the data is who they claim to be. Audit logs assess the validity and consistency of data running in the network and are important tools for verifying whether commands have been executed by legitimate users. As such, regulators must be able to consider how service providers are monitoring audit logs. Managerial procedures and operations should also be put in place to control access to customer information and understand system vulnerabilities.[4]

**Non-repudiation:** the service provider's self-protection from possible abusive behavior of consumers and employees, ensuring transaction finality and security. Ensuring that individuals agree with the terms and conditions of the service before any action and using digital signatures prevent individuals from denying their actions. Public key certificates also allow service providers to trace the origin of the transaction in case there is no direct exchange of information between entities.

These principles offer a framework for understanding vulnerabilities in MFS that is complementary to the discussion of threats and risks. Construing threats as violations of specific core management principles can help to determine the necessary regulatory response. The process of risk management helps to further formulate and calibrate that response.

### PROCESS

Risk management proceeds by 1) evaluating risks, 2) analyzing these risks by expected impact and likelihood, and 3) monitoring these risks according to expectations of impact and likelihood.

[3] A hash total is used to check the completeness and accuracy of data. If there are any changes or missing items, the new hash total will not reconcile with the original.

[4] These procedures can be used to understand the flow of information within the service provider and identify where vulnerabilities can be exploited. Moreover, it effectively identifies authorities within the service provider, making it easier to identify responsibilities in cases of accidental disclosure of information or unauthorized use. Permission controls (i.e. read, write, execute, delete) are designed based on the responsibility and authority structure. This gives tighter control in terms of data modification and fabrication.

1) **Risk evaluation.** Evaluation criteria allow potential system threats to be soundly assessed. The following criteria are suggested for MFS:

   - Feasibility of threat: Has this threat occurred already? Which components were affected? Software? Channel? How long did it take before this threat was identified?

   - Recorded incidents: How many times did this threat occur during the past 10 years? During the past five years? How many agencies were affected?

   - Availability of countermeasures: Is there an industry best practice solution available? If not, is there another way to counteract this threat?

   - Preparedness of service providers: Are policies, service level agreements, and escalation procedures being followed? How long will it take for service providers to act on this threat?

   - Susceptibility of subscribers: Are subscribers aware of such a threat? What is the likelihood that subscribers would disclose their information voluntarily upon encountering such threat? Can a subscriber easily distinguish a malicious act from a genuine one when faced with this type of threat?

2) **Risk analysis.** Risks can be analyzed by the level of impact of their consequences and by their probability of occurrence. This type of analysis will provide a set of priorities roughly ordered by expected costs. An illustration of this principle is presented in Table 2.

3) **Risk monitoring.** Once the identified risk has been mitigated, it is important that a designated team monitor its performance and evaluate it against previous experience. The team must come up with a checklist of the problems encountered before treating the risk. After treatment, the same team should monitor the stability and effectiveness of the action that was taken and carefully analyze the system for potential new threats. These observations should then be recorded alongside the original checklist and reported to business owners.

   - System auditing: a fundamental control structure that examines, verifies, and corrects faults and loopholes in certain functions of the system. Service providers are encouraged to conduct system audits regularly to ensure that system vulnerabilities are addressed and that no malicious activities are being overlooked. This is especially essential when testing the functionality of newly deployed systems.

   - Gap analysis: an extension of the checklist that was previously mentioned, this is an effective tool for differentiating performance gaps in terms of system functionality. Here it is presented in a matrix that compares current and expected performance and ranking of the analyzed component.

## Conclusion

We can now unify these discussions of MFS information flows, threats, and risks, as well as the principles and procedures used to address MFS vulnerabilities.

Any response strategy must begin by localizing the vulnerability within the network of MFS data flows. It is therefore essential that regulators have a basic grasp of the architecture of MFS systems, especially how information moves from one network element to another. With this understanding, regulators can then isolate the vulnerabilities arising from how a network element handles information. By identifying these information-handling vulnerabilities, regulators can then assess which of the threats identified in Table 1 is most likely to compromise the MFS network. The presence of any such threat violates the principles of data protection outlined in Identifying MFS Technology Risks. As a result, both financial and non-financial information are subject to specific technology risks. Risk analysis can determine which of the items indicated in the risk register is highly likely to occur and will have the greatest impact on consumers.

When populated with measures of probability and impact, the risk register orders risks by their rating (highest to lowest). With a prioritized list of risks, regulators can, tier by tier, identify the types of security controls required to mitigate these risks. These security controls will become the baseline for creating and implementing policies that address technology risks in the MFS environment. Table 3 on the following page shows a sample of how this analysis can be performed.

## Table 3. Vulnerabilities and recommended security controls

| Risk site (network element) | Threat | Principle violated | Probable risk | Recommended security controls |
|---|---|---|---|---|
| Mobile network application | • Disclosure<br>• Interception | Confidentiality | Critical information sent via SMS is read | • Customer account numbers are encrypted when transported<br>• Customer PINs are encrypted when displayed and transported |
| End-user handset | • Modification | • Integrity<br>• Authentication | Infection caused by mobile malware | • Network-side policies on information downloadable on handsets<br>• Use of anti-virus specifically for smart phones |
| SMS Center, MFS application, bank network | • Interruption | • Availability<br>• Non-repudiation | Denial-of-service attacks | • Implement a system that restricts packet response time<br>• Require MFS to establish a highly secured network environment by adapting best-practice security standards like ISO9001 |
| End-user handset | • Fabrication | • Authentication<br>• Non-repudiation | Phishing attacks | • Require an active customer awareness campaign to educate consumers about malicious messages<br>• Encourage consumers/victims to report the mobile number of malicious attackers to telecommunications service providers so that warning messages can be sent and that mobile number permanently blocked |

## References

AUJAS. 2011. Mitigating Security Risks in USSD-based Mobile Payment Applications. http://www.thectoforum.com/content/mitigating-security-risks-ussd-based-mobile-payment-applications. [Accessed 26 July 2011].

BEVIS, J. 2007. Disaster Recovery – Alternate Site Geographical Distance. http://infosecalways.com/2007/12/19/disaster-recovery-%E2%80%93-alternate-site-geographical-distance./ [Accessed 24 July 2011].

BOCAN, V. & CREDU, V. 2006. Mitigating Denial of Service Threats in GSM Networks. In: GSM, C.A.P.I. (ed.).

DEPARTMENT OF PREMIER AND CABINE. 2009. Tasmanian Government Information Security Guideline. http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0004/89185/Information_Security_Guidelines.pdf [Accessed 23 July 2011].

DHILLON, G. 2007. Principles of Information Systems Security: Text and Cases. John Wiley & Sons Inc.

GOSTEV, A. 2006. Mobile Malware Evolution: An Overview, Part 1. SECURELIST [Online].

HICKS, S. 2006. Mobile and Malicious: Security for mobile devices getting critical: best practices and technologies. Enterprise Networks & Servers [Online].

JUUL, N.C. 2002. Security Issues in Mobile Commerce using WAP. http://medusa.sdsu.edu/network/security/wap-bled.pdf.

LEE, P. 2002. Cross-site scripting http://www.ibm.com/developerworks/tivoli/library/s-csscript/ [Accessed 26 July 2011].

PELTIER, T. 2001.Information Security Risk Analysis. In: ASSET IDENTIFICATION: NETWORK AND SOFTWARE, P. A. O. A. (ed.). CRC Press LLC.

SAHIBUDIN, S., SHARIFI, M. & AYAT, M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Service providers. IEEE Computer Society, 749-754.

ZROBOK, D. 2001. The Security Issues with WAP. http://hygelac.cas.mcmaster.ca/courses/SE-4C03-01/papers/Zrobok-WAP.html [Accessed 26 July 2011].

## About AFI Mobile Financial Services Working Group Guideline Notes

The AFI Mobile Financial Services Working Group guideline notes are based on the experience of group members and attempt to provide guidance on the definition of common standards, approaches, and practices for MFS regulation and supervision within AFI member institutions. The notes are not summaries of best practices nor do they propose new principles or revisions to existing core principles. Instead, they highlight key MFS policy and regulatory issues and identify challenges to be addressed. The definitions here are intended to complement rather than replace similar MFS definitions drafted by International Standard Setting Bodies (SSBs).

## About AFI

The Alliance for Financial Inclusion (AFI) is a global network of financial inclusion policymaking bodies, including central banks, in developing countries. AFI provides its members with the tools and resources to share, develop and implement their knowledge of financial inclusion policies. We connect policymakers through online and face-to-face channels, supported by grants and links to strategic partners, so that policymakers can share their insights and implement the most appropriate financial inclusion policies for their countries' individual circumstances.

Learn more: www.afi-global.org

**Alliance for Financial Inclusion**

**AFI,** 399 Interchange Building, 24th floor, Sukhumvit Road, Klongtoey – Nua, Wattana, Bangkok 10110, Thailand
**t** +66 (0)2 401 9370 **f** +66 (0)2 402 1122 **e** info@afi-global.org www.afi-global.org
www.facebook.com/AFI.History @NewsAFI

AFI is funded by the Bill & Melinda Gates Foundation and administered by GIZ (German International Cooperation)