CYBERSECURITY FOR MOBILE FINANCIAL SERVICES

FAQs for regulators, supervisory authorities and digital financial services providers

October 2018

Photo: Sudipto Das

Logistics

1. This is an audio broadcast. Attendee microphones will remain muted during the entire webinar session.
2. To ask questions during the webinar, please use the **chat box** on the right-hand side of the Webex session. Please submit your question at any time during the webinar presentation.
3. To ensure your question is seen by the moderator, select "**All Participants**" from the drop down menu when sending your question.
4. The webinar recording will be emailed to all attendees and registrants.

Speakers

David Medine

Senior Advisor,

CGAP

Paul Makin

Financial Inclusion and
Digital Identity Consultant

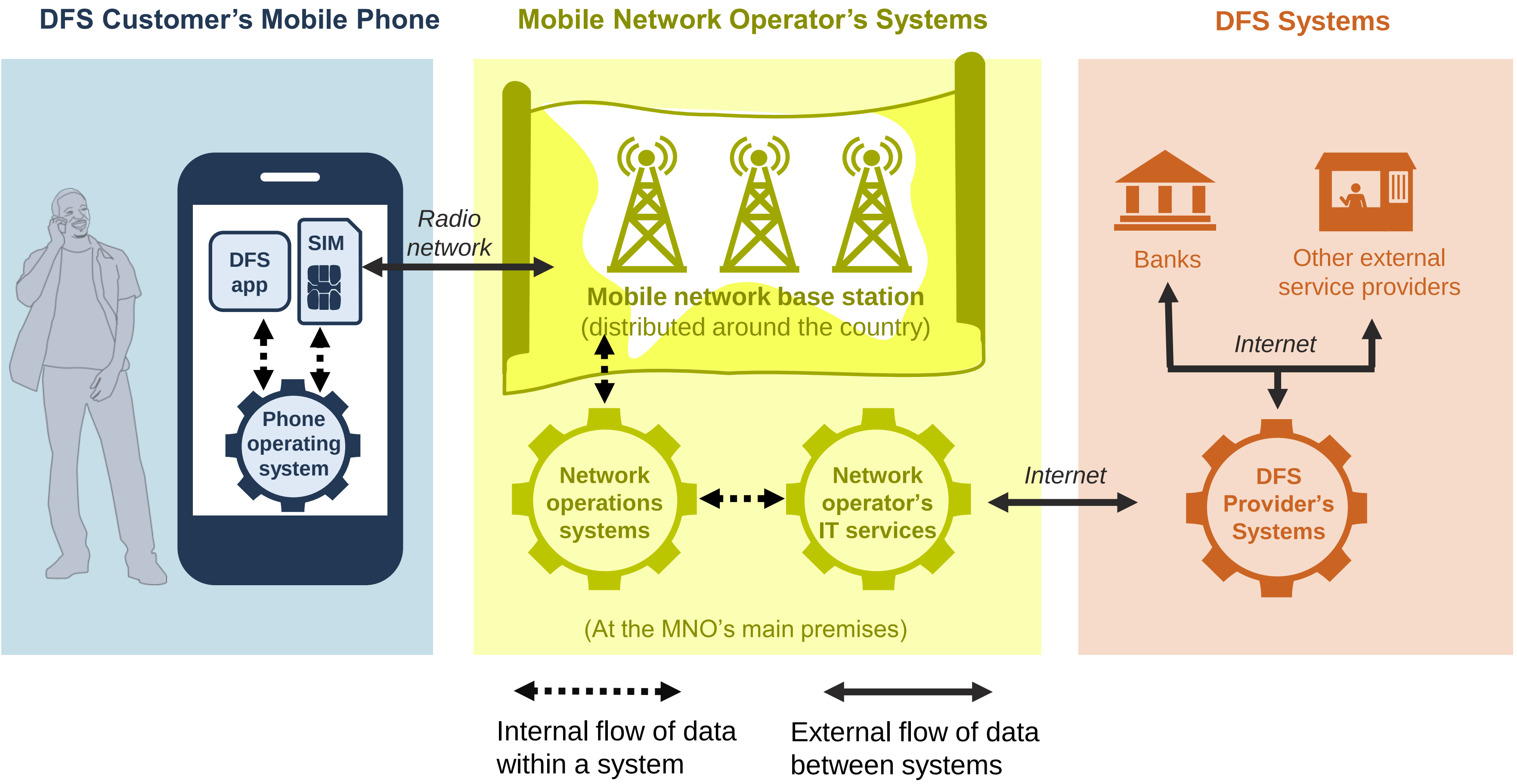
Agenda

1	Introduction: Fraud in mobile financial services
2	Are mobile networks secure enough for financial services?
3	Are mobile phones secure enough for financial services?
4	How can DFS providers secure their systems and transactions?
5	What can regulators and supervisors do to ensure the security of DFS systems?
6	Recommendations

Introduction: Fraud in mobile financial services

Photo: AJ Rudin

Introduction: Fraud in mobile financial services



DFS Customer's Mobile Phone

DFS app

SIM

Phone operating system

Radio network

Mobile Network Operator's Systems

Mobile network base station
(distributed around the country)

Network operations systems

Network operator's IT services

(At the MNO's main premises)

Internet

DFS Systems

Banks

Other external service providers

Internet

DFS Provider's Systems

Internal flow of data within a system

External flow of data between systems

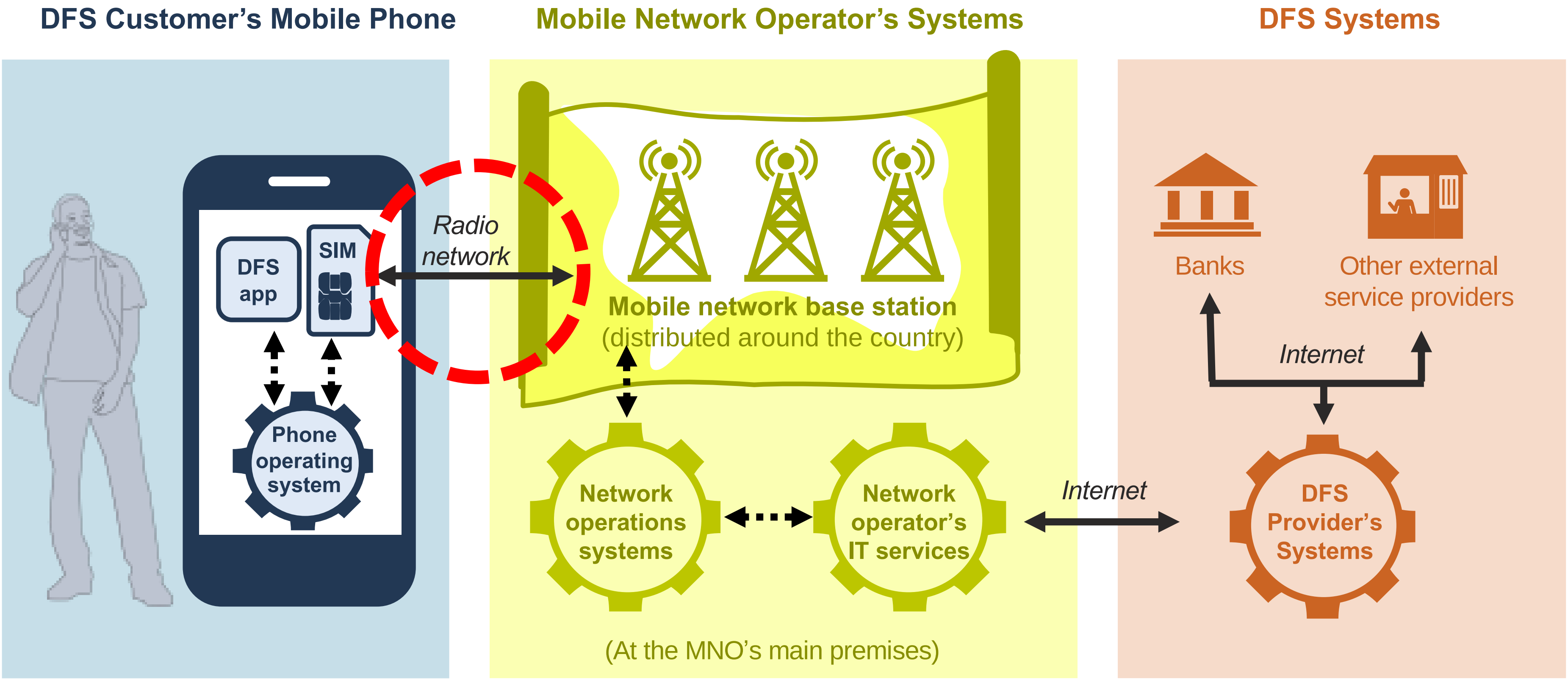
Are mobile networks secure enough for financial services?

CGAP

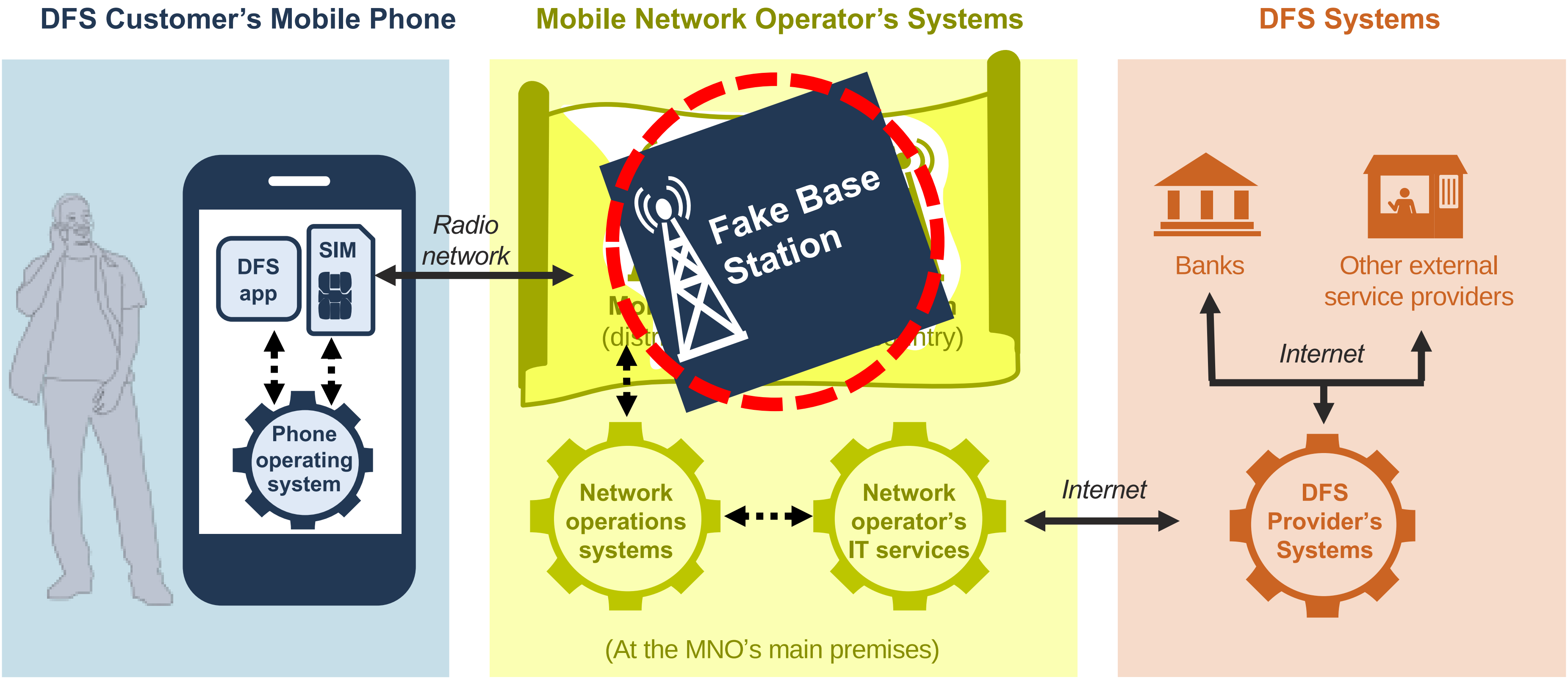
Mobile network security

1. Eavesdropping by external hackers
2. Eavesdropping via fake network base stations
3. Exploitation of roaming
4. Insider eavesdropping
5. Other insider threats

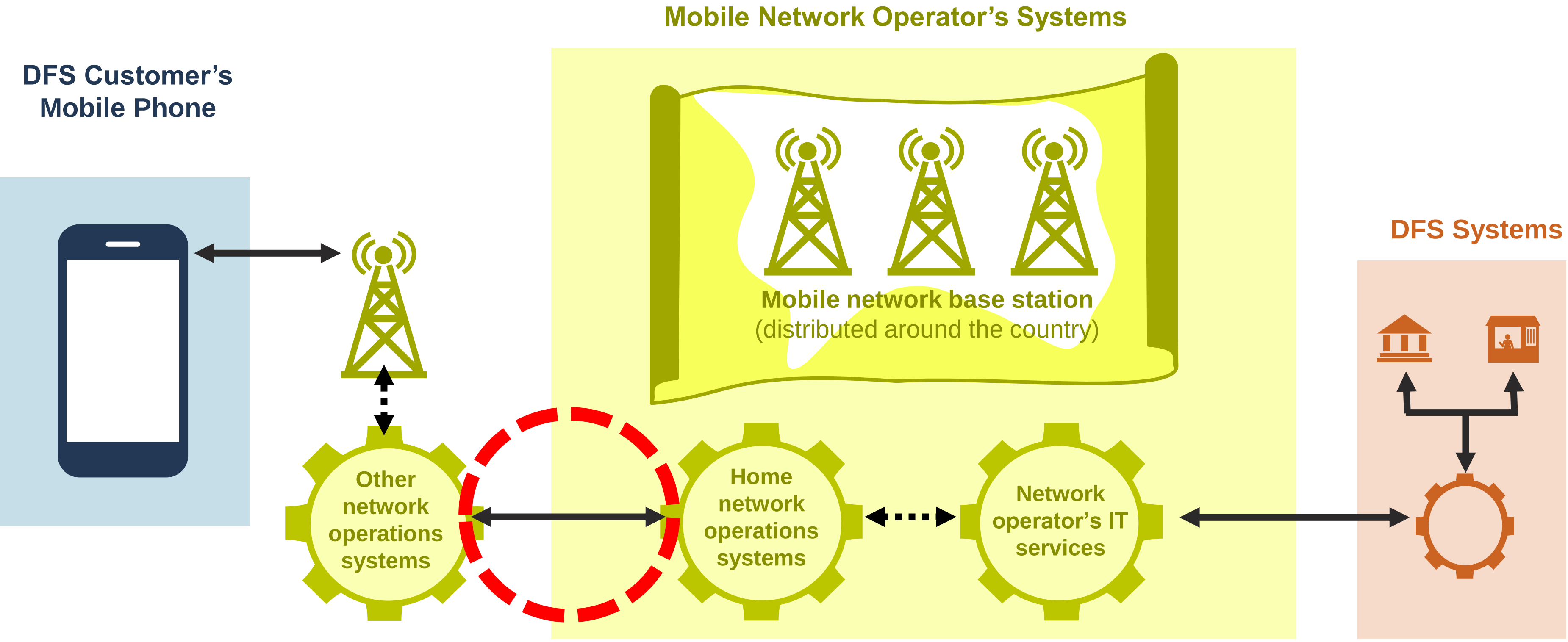
1. Eavesdropping by external hackers


DFS Customer's Mobile Phone
Mobile Network Operator's Systems
DFS Systems
DFS app
SIM
Phone operating system
Radio network
Mobile network base station
(distributed around the country)
Network operations systems
Network operator's IT services
(At the MNO's main premises)
Internet
Banks
Other external service providers
Internet
DFS Provider's Systems

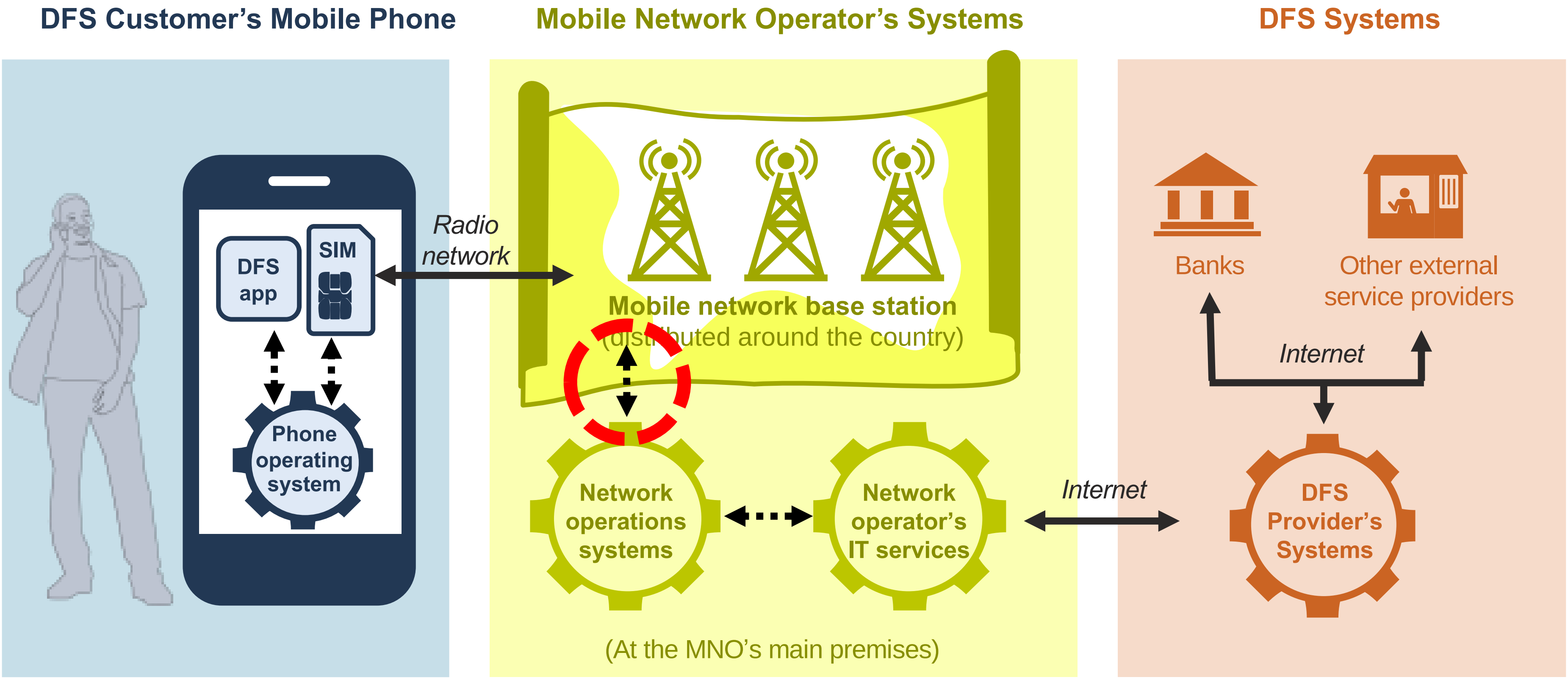
2. Eavesdropping via fake stations


DFS Customer's Mobile Phone
Mobile Network Operator's Systems
DFS Systems
DFS app
SIM
Phone operating system
Radio network
Fake Base Station
(dist
ntry)
Network operations systems
Network operator's IT services
(At the MNO's main premises)
Internet
Banks
Other external service providers
Internet
DFS Provider's Systems

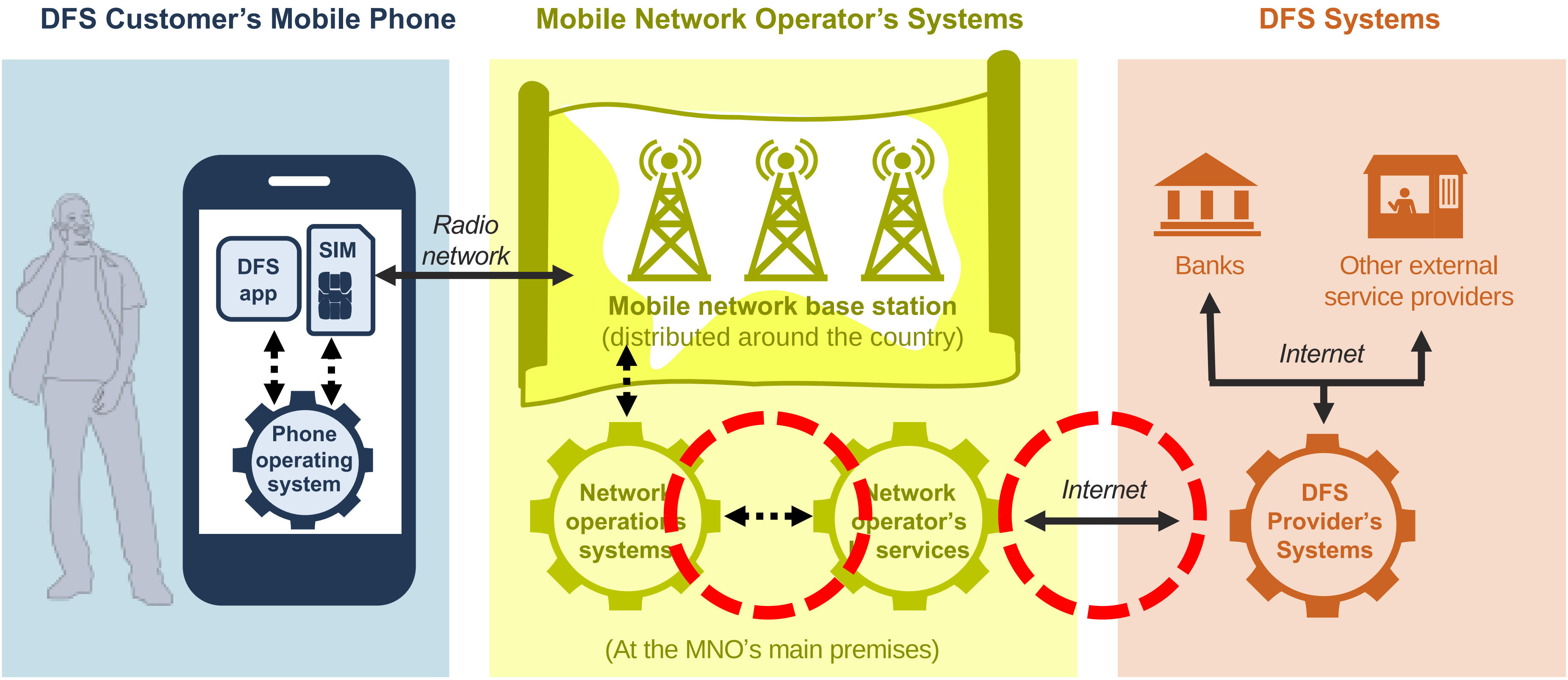
3. Exploitation of roaming


Mobile Network Operator's Systems
DFS Customer's Mobile Phone
Mobile network base station
(distributed around the country)
DFS Systems
Other network operations systems
Home network operations systems
Network operator's IT services

4. Insider eavesdropping


DFS Customer's Mobile Phone
Mobile Network Operator's Systems
DFS Systems
DFS app
SIM
Phone operating system
Radio network
Mobile network base station
(distributed around the country)
Network operations systems
Network operator's IT services
(At the MNO's main premises)
Internet
Banks
Other external service providers
Internet
DFS Provider's Systems

5. Other insider threats

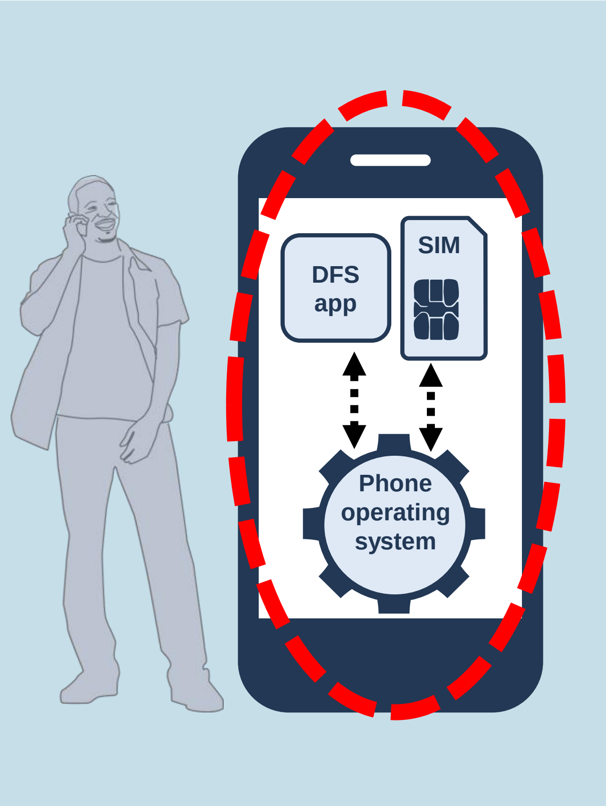

DFS Customer's Mobile Phone
Mobile Network Operator's Systems
DFS Systems
DFS app
SIM
Phone operating system
Radio network
Mobile network base station
(distributed around the country)
Network operations systems
Network operator's services
Internet
(At the MNO's main premises)
Banks
Other external service providers
Internet
DFS Provider's Systems

Importance of mobile network security

Photo: Trung Vo Chi

Are mobile phones secure enough for financial services?

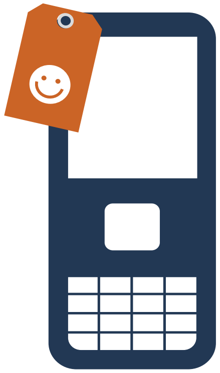
Mobile phone security



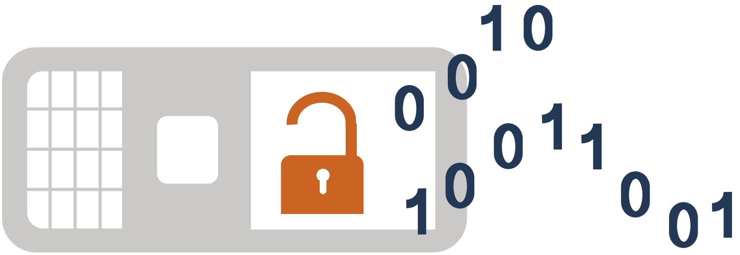
- Mobile phones are an important element in ensuring security and confidentiality of customers’ money.
- Properly securing mobile phones requires action from DFS providers **and** phone manufacturers.
- Customers need to know how best to safeguard their money.

Feature phones

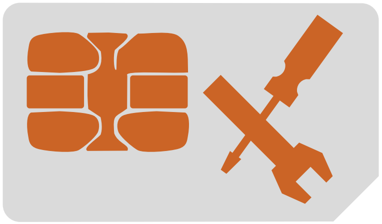
Affordable



Phones themselves not a target for hackers



Can’t be used to enhance security of transactions



Except with a **SIM Toolkit app**; otherwise enhanced transaction monitoring is essential

Smartphones

Smartphones are sophisticated computers connected to mobile networks that are built from the ground up with security in mind. Nonetheless, flaws still occur.

- **Smartphone manufacturers** should make fixes available whenever a flaw is found.
- **Smartphone owners** should update their phone's software as soon as a new version is available.

DFS providers should never allow devices with compromised security to access their services.

How to make phones more secure

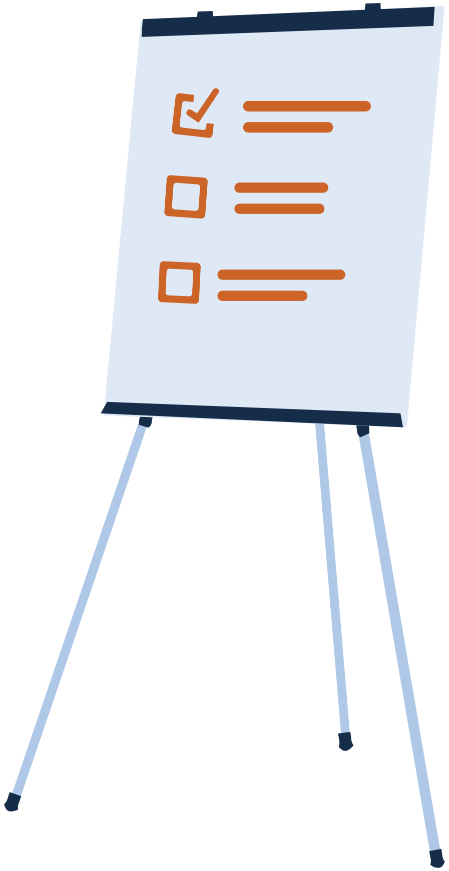
DFS customers should:

- Secure their phones, and install updates.

DFS providers should:

- Offer an app.
- Control access to the app.
- Update the app to address security issues.

DFS smartphone app developers should adopt the well-understood technical approaches to this problem.



CGAP

App-based transactions have fewer vulnerabilities

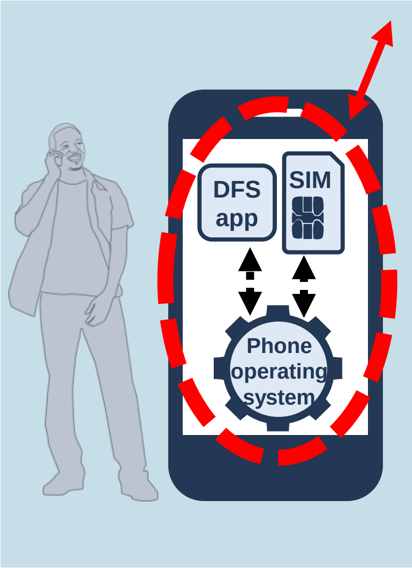
USSD has major security vulnerabilities

SMS is little better

Smartphone apps are the best option – but not always available

No DFS provider should rely on the security of the mobile network or the mobile phone.

Best practice is to provide their own end-to-end security.

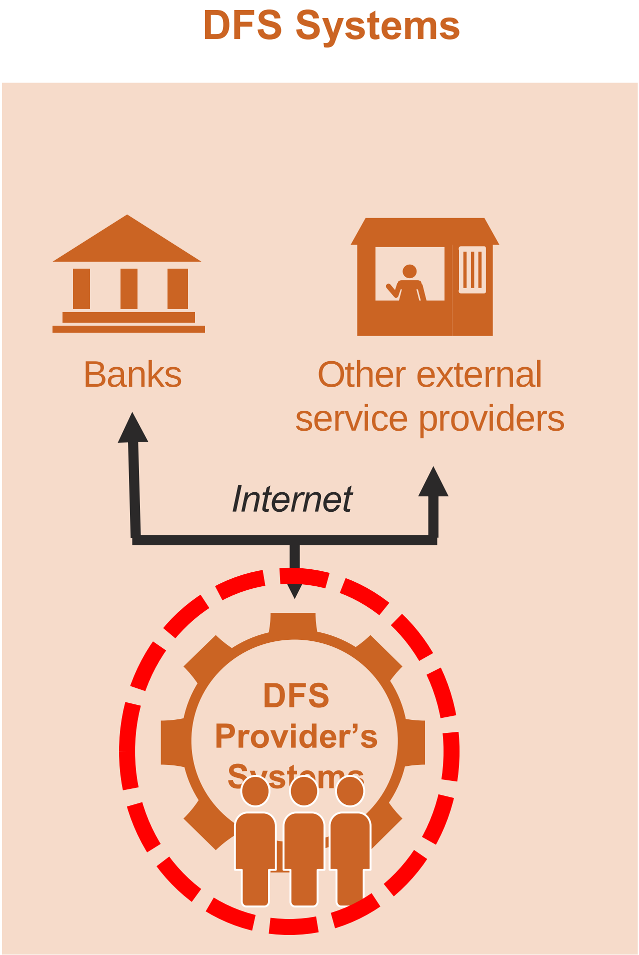


How can DFS providers secure their systems and transactions?

Focus on insider threats first

The most successful attacks in terms of the total value of money defrauded are insider jobs.

DFS providers' cybersecurity efforts should **focus on insider threats first.**



How to mitigate insider threats

Tip 1: Know your staff

Cybersecurity can be undermined by malicious staff.

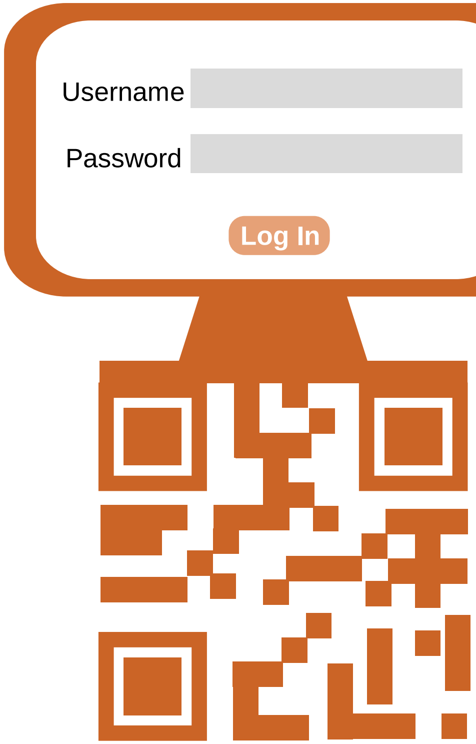
Background checks should be made on all key staff.

How to mitigate insider threats

Tip 2: Staff authentication

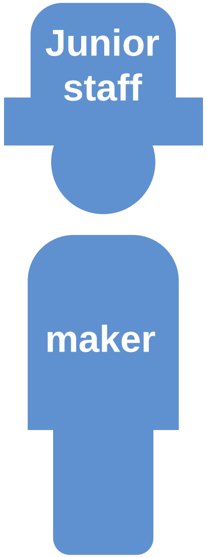
Internal controls are only effective if staff members can be reliably identified and if their interactions with the DFS platform can be controlled.

- **Two-factor authentication for staff login**
- **Record all login attempts**



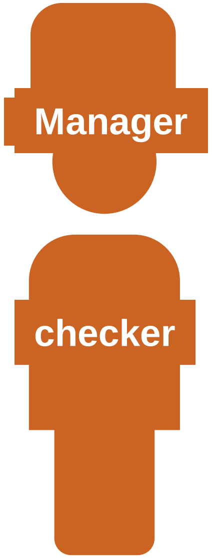
How to mitigate insider threats

Tip 3: Role-based access and auditability



Money transfer functions should be carefully controlled through:

- **Role-based access**
- **Maker/checker controls**

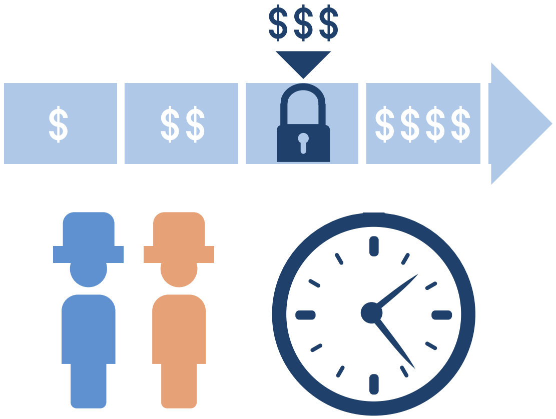


How to mitigate insider threats

Tip 4: Processes and control points

Carefully defined and implemented business processes are an essential part of cybersecurity:

- Use a **business process management service**
- Include a set of **control points**



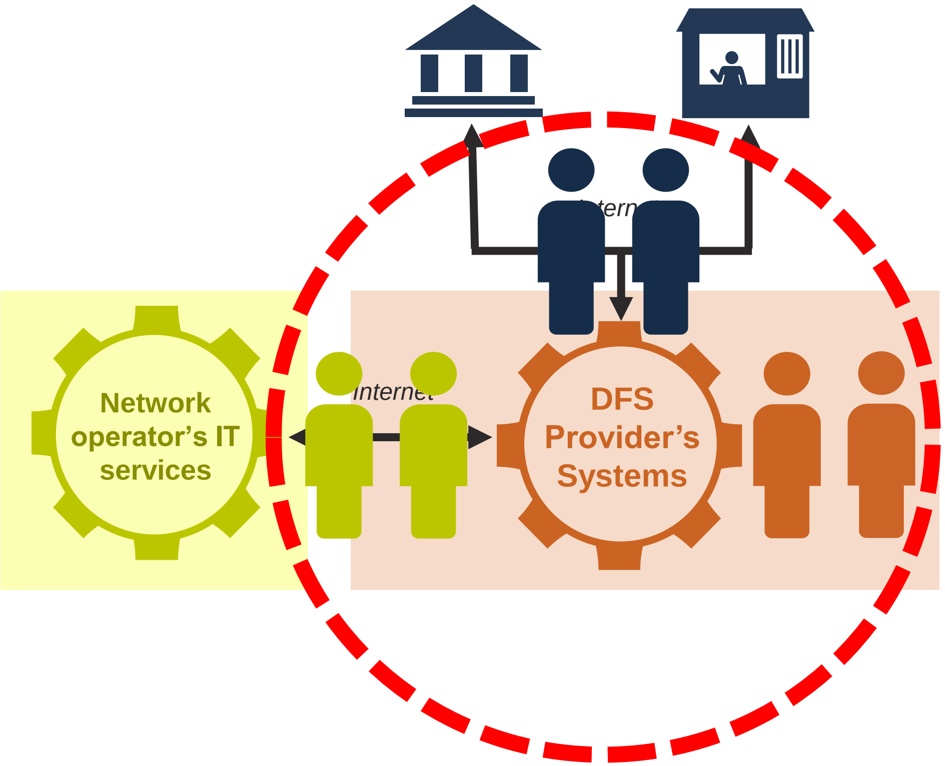
How to mitigate insider threats

Tip 5: Regular reconciliation of accounts

Reconciliation has two main functions:

- Ensure all customer balances are secured by real funds in a bank account.
- Indicate potential fraud perpetrated by breaching cybersecurity controls and controls for the creation of value.

Adopt measures to protect against third-party threats



How to mitigate insider and third-party threats

Tip 1: Know your suppliers

It is important that DFS providers verify the integrity of their suppliers and understand the risks that arise from suppliers' internal activities or their relationships with third parties.

CGAP

How to mitigate insider and third-party threats

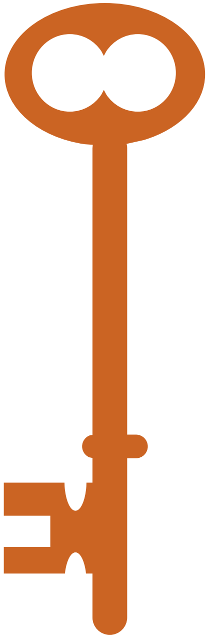
Tip 2: Encryption

Cryptography is crucial for the operation of DFS and for data protection and privacy.

It helps ensure the confidentiality and integrity of communications.

All data must be encrypted **in transit and at rest**.

All transactions and staff activities **must be logged** for future auditing or investigations.



How to mitigate insider and third-party threats

Tip 3: Active, automated transaction monitoring

Implement transaction monitoring.

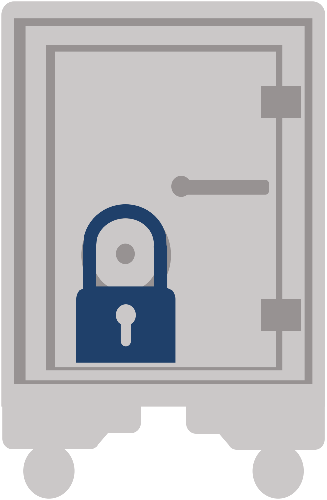
Appoint a fraud officer.

Leverage transaction investigation tools for rapid investigation of potential crimes.

How to mitigate insider and third-party threats

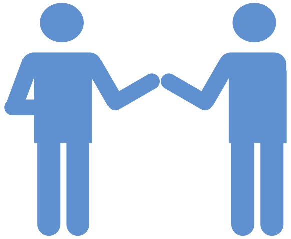
Tip 4: Physical security

Physical security limits the opportunity for the subversion of cyber-controls.



Well-managed data centers **focus equally on physical and cybersecurity**.

This applies also to visitors.



CGAP

How to mitigate insider and third-party threats

Tip 5: Cybersecurity reviews

Every DFS service should undergo an external cybersecurity review.

Supervisors should have sight of the results.

What can regulators and supervisors do to ensure the security of DFS systems?

CGAP

Should regulators allow DFS?

Yes, but they should require certain security measures.

The aspiration should be a service that provides its own end-to-end, industrial-grade security

In most lower-income countries, we recognize that this is not possible.

Additional measures are necessary when a service relies on USSD.

Create an expert body to issue and update security standards

Financial sector regulators should **not** attempt to set technical standards for DFS cybersecurity management.

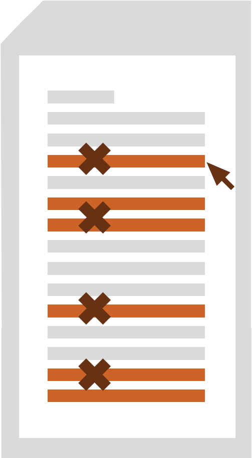
Instead of technical standards, regulators should specify:

- An expert body that issues security standards.
- Requirements to conform to those standards
- An inspection/audit regime
- A mechanism for responding to new threats

Consider liability of DFS providers

DFS providers' liability

Regulators should consider the liability issues that might arise if security standards are not followed, especially if noncompliance results in financial loss.



Regulators may allow lower technical security standards (including, for example, USSD) by balancing the higher risk with stricter liability.

Consider responsibilities of supervisors

Supervisory authorities have a data security responsibility, too.

Sensitive data supplied by DFS providers to the supervisory authorities, including data about their customers, should be subject to many of the same internal cybersecurity measures that are required of DFS providers.

Recommendations

Regulators

- Identify a center of cybersecurity excellence; national, regional or international.
- Work with this center to define technical cybersecurity standards for the delivery of mobile financial services.
- Obtain a commitment that those standards will be maintained and updated as new cybersecurity threats emerge and technology advances.
- Define policy that references these standards.

Supervisory authorities

- Engage DFS providers in a program of continuous improvement.
- **Adopt a comprehensive data security supervisory program**, including
  - Monitor DFS providers' compliance with cybersecurity regulations.
  - Require annual cybersecurity review reports from DFS providers.
  - Visit DFS providers' operational centers to verify that the process and control points that have been documented are being followed.
  - Review and compare suspicious transaction reports (STRs) received from DFS providers.

DFS providers

- Assess risk exposure and improve countermeasures where necessary.
- Annually engage a qualified third-party to carry out a risk assessment and cybersecurity review. Submit report to supervisory authorities.
- Focus equally on technological controls and process controls.
- Engage regularly with supervisory authorities as part of a program of continuous improvement.
- When assessing liabilities to customers, give reasonable consideration to any identified security weaknesses and consequent issues around fairness to customers.

Questions and Answers

Please use the chat box to send us your questions. Be sure to send them to "All Participants" so everyone can see. Thanks!

CGAP

Stay connected with CGAP

www.cgap.org

@CGAP

Facebook

LinkedIn

CGAP

AFD

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG

BILL & MELINDA
GATES *foundation*

AGENZIA ITALIANA
PER LA COOPERAZIONE
ALLO SVILUPPO

npm

USAID
FROM THE AMERICAN PEOPLE

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Global Affairs
Canada

IFAD
Investing in rural people

UKaid

Sida

mastercard
foundation

KOICA
Korea International
Cooperation Agency

giz

Federal Ministry
for Economic Cooperation
and Development

UN
CDF

Ministry of Foreign Affairs of the
Netherlands

Australian Government
Department of Foreign Affairs and Trade

FMO

IDB

Italian Development
Cooperation
Ministry of Foreign Affairs
and International Cooperation

Norad

CDC
Investment works

Citi Foundation
citi

UN
DP

ON
OMIDYAR NETWORK™

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development
and Cooperation SDC

KFW

European
Investment
Bank

Michael & Susan Dell
FOUNDATION

MetLifeFoundation

•cdp•

OMIN

UDENRIGSMINISTERIET
MINISTRY OF FOREIGN AFFAIRS OF DENMARK

IFC
International
Finance Corporation