CYBERSECURITY FOR MOBILE FINANCIAL SERVICES

FAQs for regulators, supervisory authorities and digital financial services providers

CGAP

August 2018

Photo: Sudipto Das

Preface

Today, nearly 80 percent of the developing world's population owns a mobile phone. As mobile phones have become common in low- and middle-income countries, they have become effective delivery channels for financial services to poor people, especially those living in rural and remote areas that lack financial services infrastructure.

However, mobile financial services can put consumers at risk of fraud if proper cybersecurity measures are not in place. The risk is heightened in developing countries, where consumers rather than providers generally bear the cost of fraud. Mobile financial services can meaningfully advance financial inclusion, but to do so they must be reliable and trustworthy.

This slide deck answers some of the most frequently asked questions regulators, supervisors, mobile network operators (MNOs), and digital financial services (DFS) providers have about vulnerabilities in mobile financial services and countermeasures that can be taken to address data security.

Contents

This deck provides an overview of cybersecurity issues in mobile financial services. It addresses the security of DFS provider's own systems and services as well as the security of the mobile networks they use to deliver their services, the security of the phones that customers use to access their services, and the implications this might have for the security of the overlaid mobile financial service, and of the customers' personal data and finances.

In addition, the deck provides regulatory and supervisory authorities with the information they need to assure themselves of the cybersecurity of the services they oversee; and to highlight to DFS providers all of those areas they should be considering. That said, this is not, and cannot be, an exhaustive list. It is instead a jumping off point for more thorough investigations.

Contents

Introduction: Fraud in mobile financial services

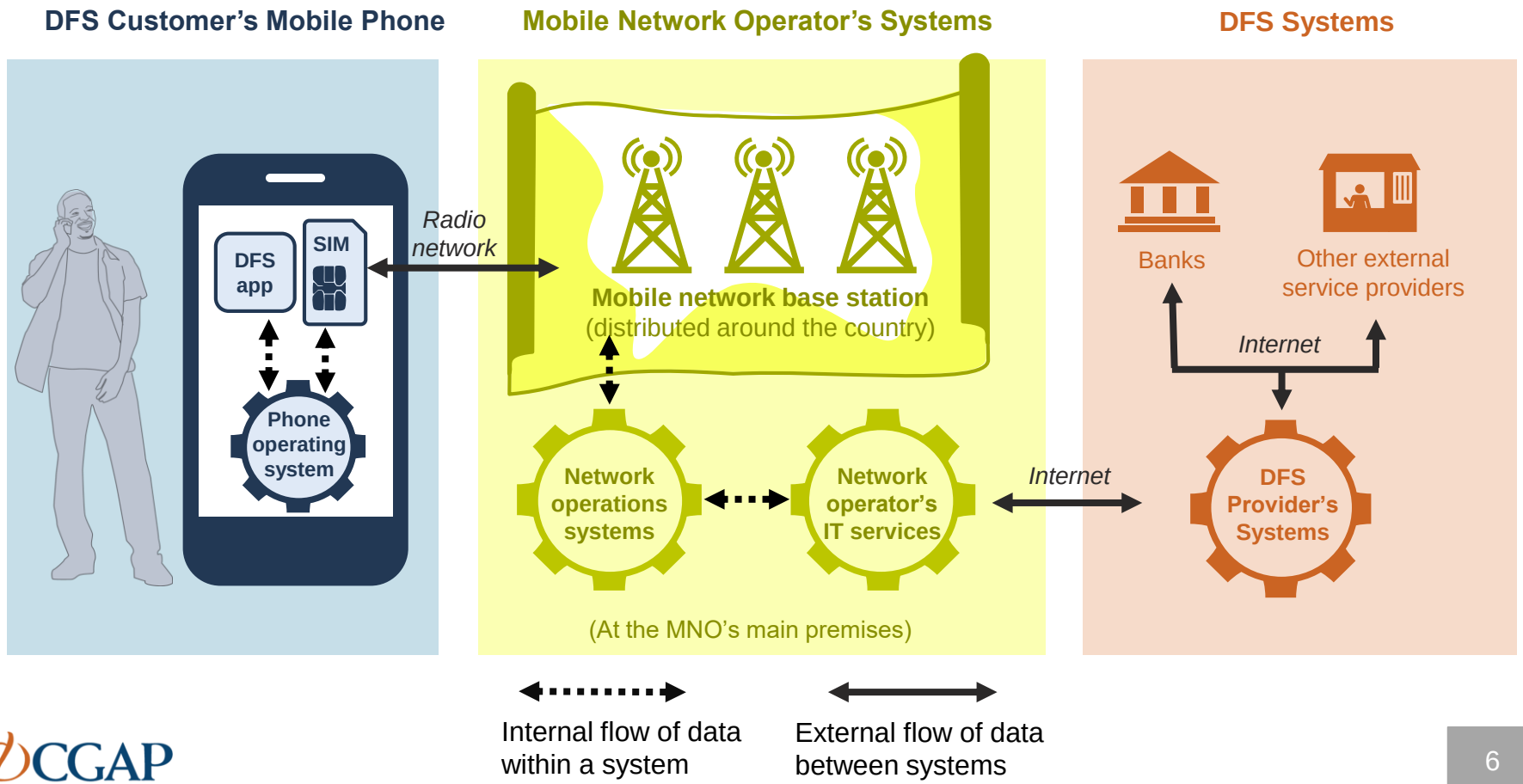
When Jonathon glanced at his mobile phone, he noticed the words “NO SERVICE” on the screen. This didn’t worry him since his mobile network occasionally went down. A few minutes later, his phone reconnected to the network and he thought all was well.

Later that day, he decided to use his mobile money account to buy a cup of coffee, but the payment failed. When he checked his balance, he found that the entire amount he thought was in his account — just yesterday, he had more than $100 — was gone.

Photo: AJ Rudin

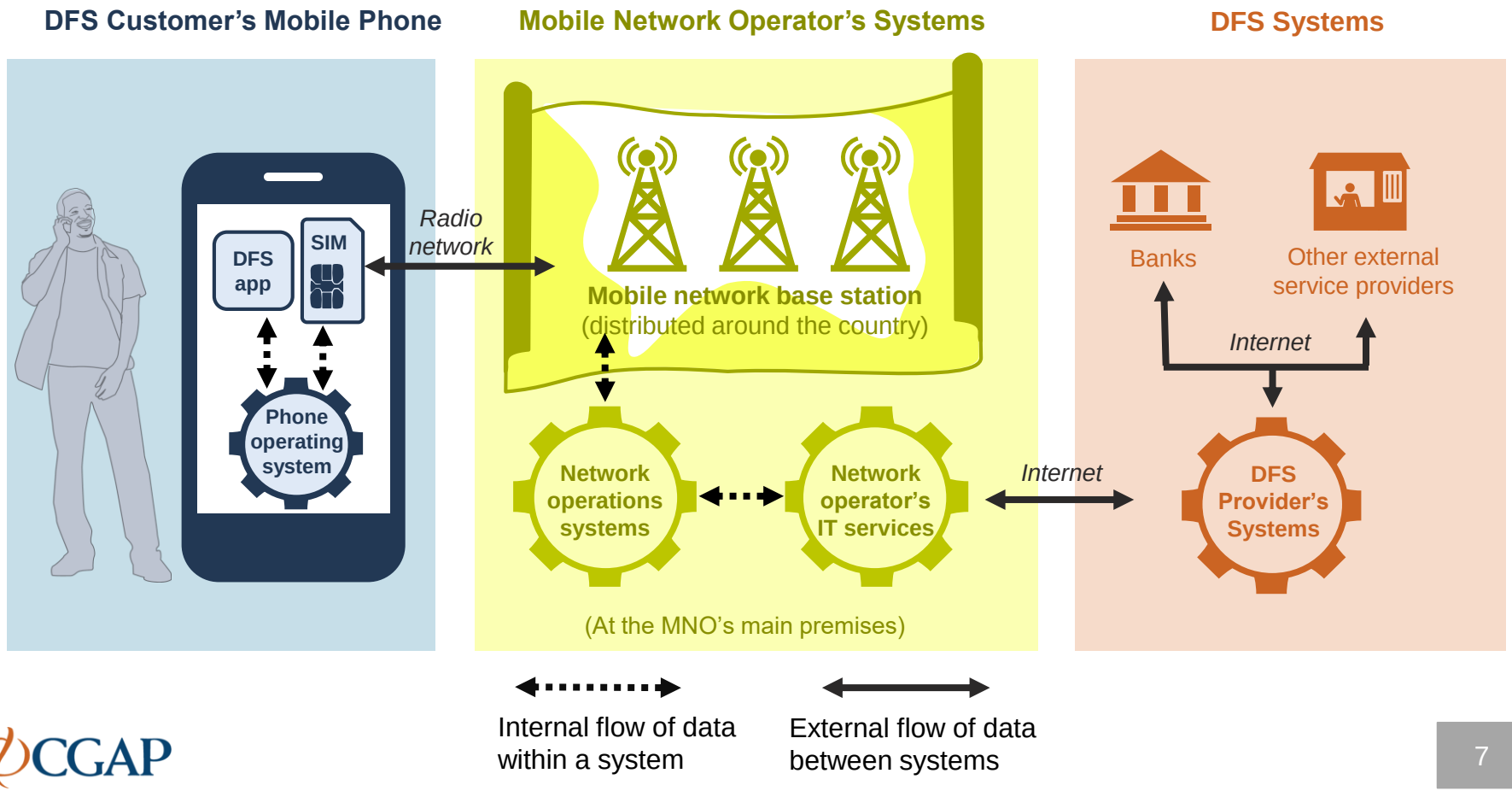
Introduction: Fraud in mobile financial services

In Jonathon's case, someone attacked the MNO's systems to deplete his account. But criminals can exploit numerous vulnerabilities in the life cycle of a mobile-based financial transaction, as financial information flows across multiple systems that may not be adequately secured.



Introduction: Fraud in mobile financial services

By answering frequently asked questions about cybersecurity in mobile financial services, we will look at key vulnerabilities along a financial transaction's journey through these systems, starting with the mobile network.



Are mobile networks secure enough for financial services?

CGAP

Mobile network security

Before a consumer's financial information passes through the mobile network to the DFS provider, it is already vulnerable to several types of attacks.

1

Eavesdropping by external hackers

Hackers intercept communications between a mobile phone and a cell tower.

2

Eavesdropping via fake network base stations

A fake mobile network disguised as a legitimate one allows criminals to intercept communications to cell towers.

3

Exploitation of roaming

A mobile network's roaming service is misused to launch attacks from anywhere in the world.

4

Insider eavesdropping

MNO staff and contractors listen to communications between cell towers and an MNO's systems.

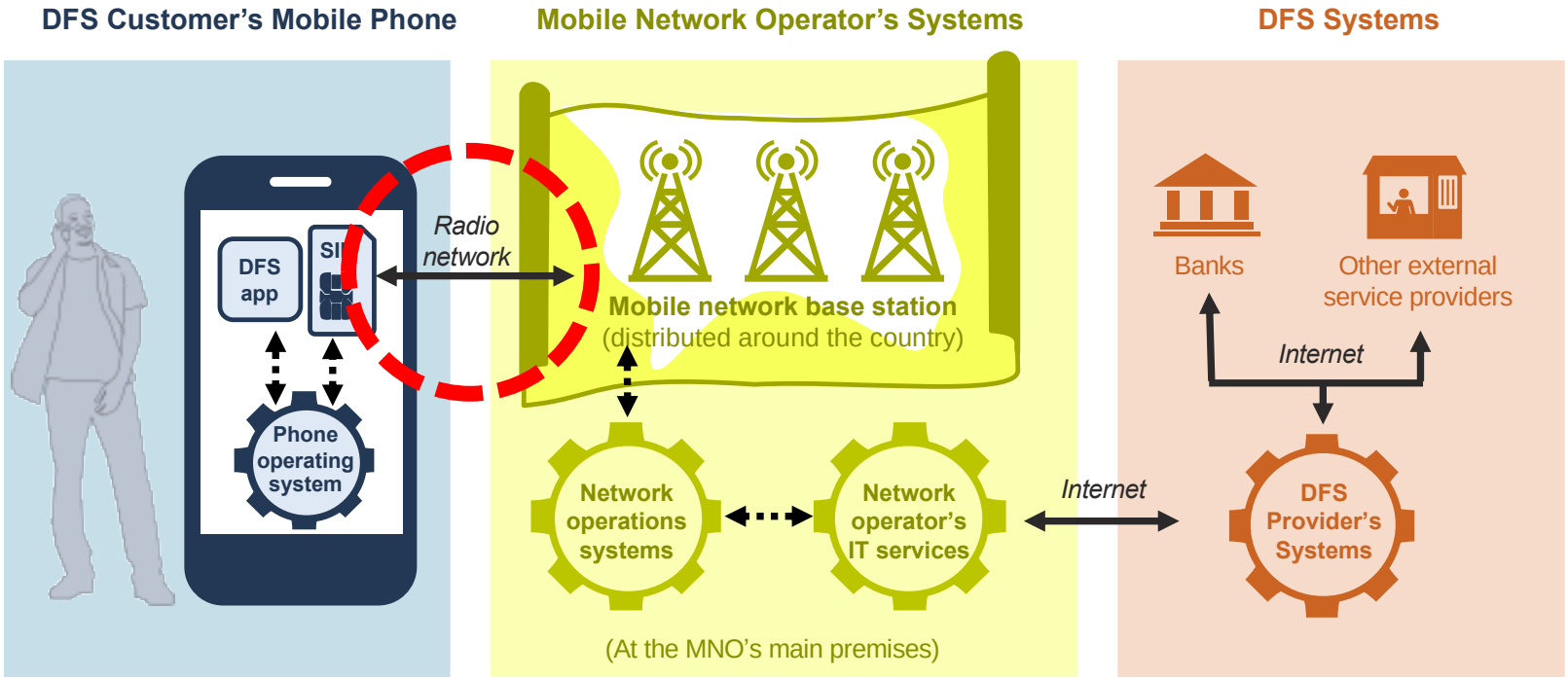
5

Other insider threats

Sophisticated criminals inside an MNO or DFS provider eavesdrop on communications between internal systems.

CGAP

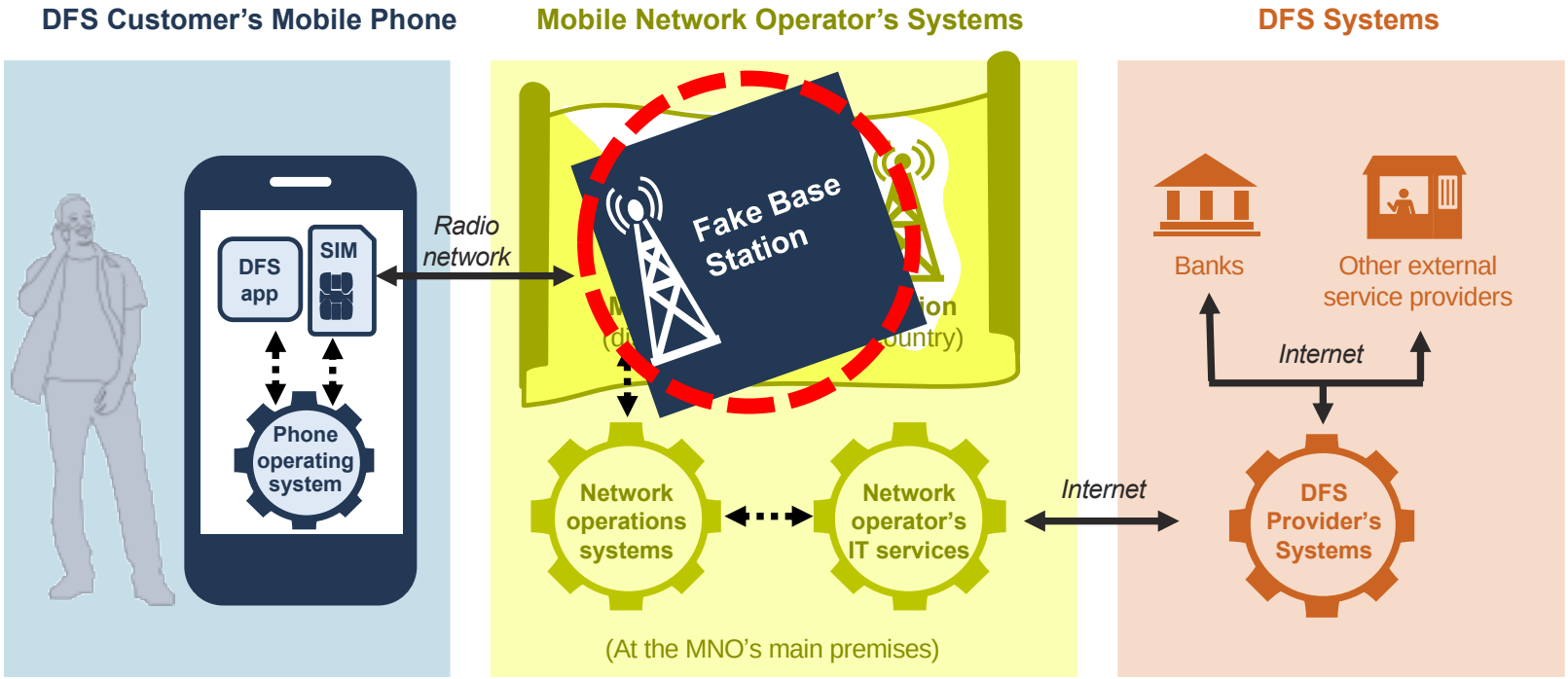
1. Eavesdropping by external hackers



HOW IT WORKS: Eavesdropping by External Hackers

External criminals intercept communications between DFS customers' mobile phones and a cell tower, including calls, text messages, USSD sessions, and mobile data, including PINs and passwords. Then, they use customers' login credentials in SIM swaps or other attacks to initiate fraudulent financial transactions. This is a localized attack limited to customers connected to a particular cell tower. It allows hackers to view, but not alter, transactions.

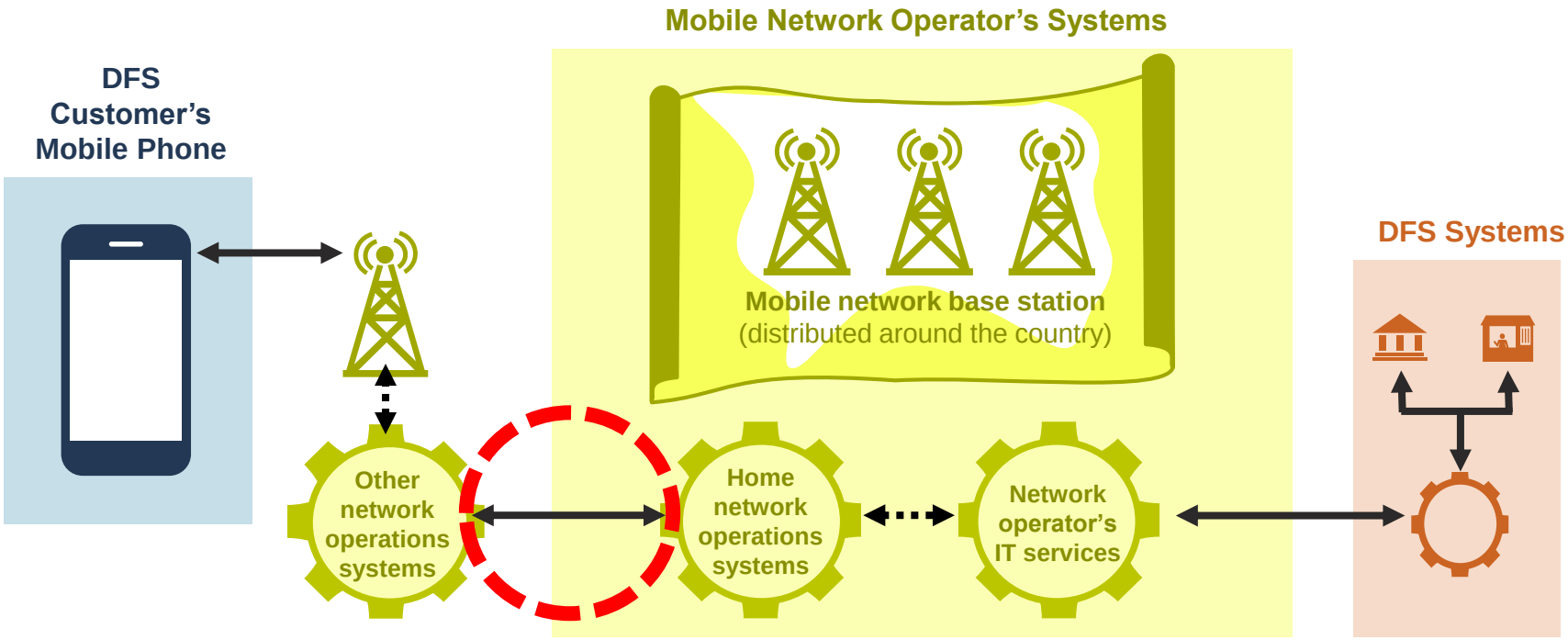
2. Eavesdropping via fake stations



HOW IT WORKS: Eavesdropping Through Fake Network Base Stations

External criminals route financial transactions through fake base stations that look like real ones to customers' phones. If the fake station's signal is stronger than the real station's (usually because it's closer to a customer), it can capture the customer's DFS session. When this happens, criminals can view and change transaction recipients and amounts. They can also steal PINs and passwords and use them later in SIM swaps or other attacks to request transactions from customers' accounts. This is also a localized type of attack.

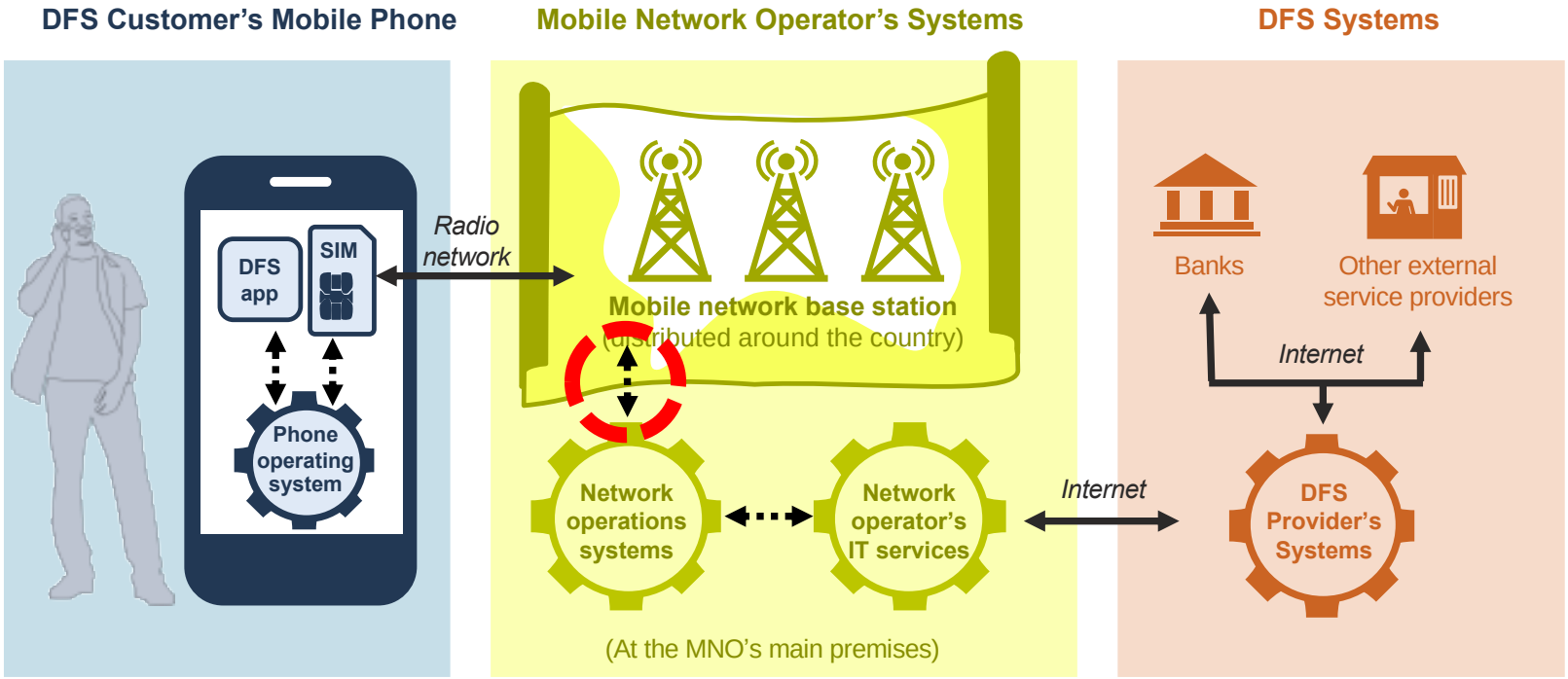
3. Exploitation of roaming



HOW IT WORKS: Exploitation of Roaming

When customers use roaming services, they connect to their home network via another MNO's network. Exploiting the links between MNOs that facilitate roaming, an external attacker can impersonate an MNO or DFS provider by sending and intercepting text messages, pushing USSD sessions to customers, or listening to voice calls. These tactics can be used to get a customer to change their PIN (which can be captured using one of the other methods discussed) or to capture a one-time PIN sent via SMS, allowing a DFS account to be hijacked.

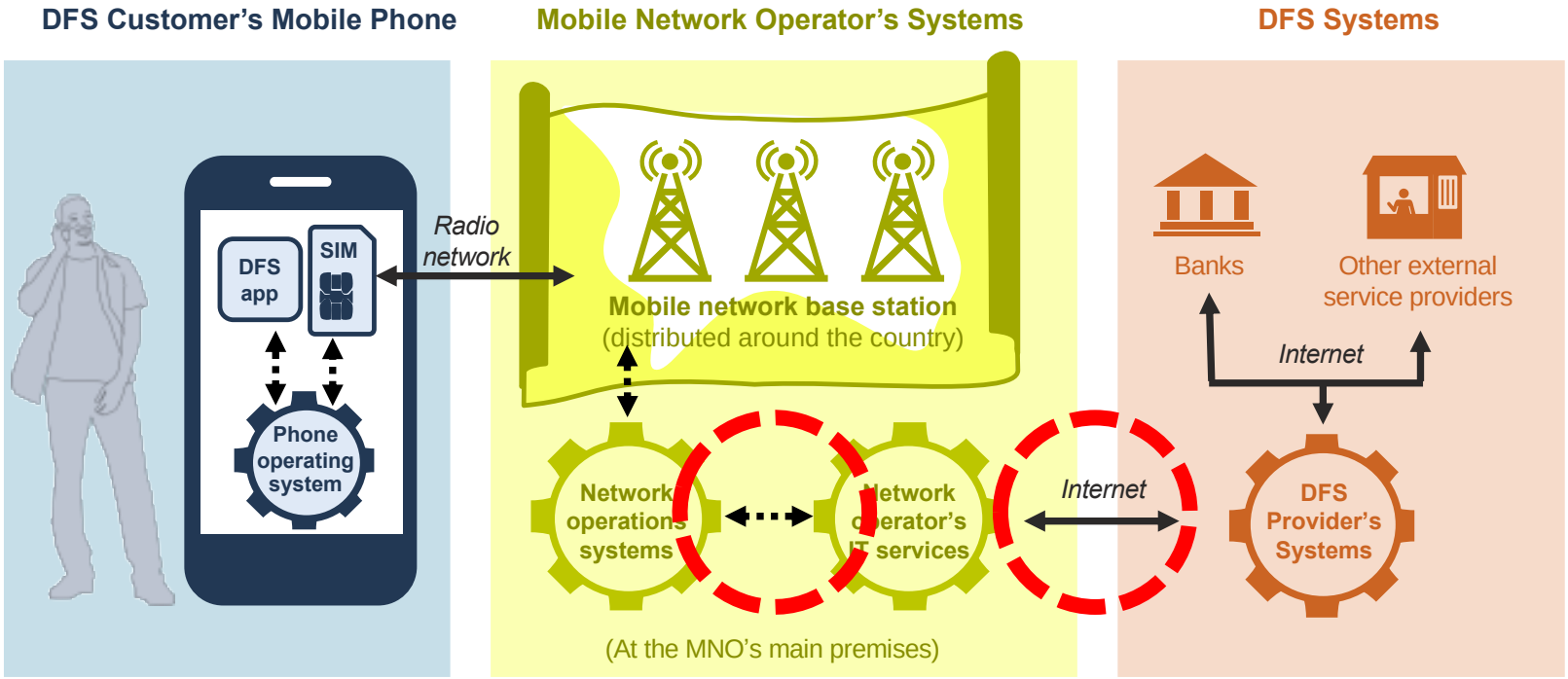
4. Insider eavesdropping



HOW IT WORKS: Insider Eavesdropping

MNO staff and contractors are able to conduct centralized attacks that simultaneously affect all DFS customers using a mobile network. They can intercept calls, text messages, USSD sessions, and mobile data sessions, and then use stolen PINs and passwords to initiate financial transactions from customers accounts. Because MNO insiders can see the activities of all their customers, rather than just individuals or those connected to a particular tower, they can identify and target an MNO's wealthiest customers for attacks.

5. Other insider threats



HOW IT WORKS: Other Insider Threats from MNOs and DFS Providers

Insiders at MNOs or DFS providers can intercept communications within and between MNOs' and DFS providers' systems, including text messages, USSD sessions, and mobile data sessions. Attackers can obtain customers' PINs and passwords and use them in SIM swaps or other attacks to request transactions from customers' accounts. These centralized attacks can simultaneously target all of a DFS provider's customers who are using a particular mobile network.

Importance of mobile network security

Criminals can attack mobile networks in many ways, potentially reducing the reliability of mobile financial services. However, this does not mean that DFS providers should stop using mobile networks to reach their customers.

Instead, they should implement strong security measures. They should never rely on someone else (i.e., the MNO) to do this for them. Later sections of this deck set out minimum protections to improve the security of financial transactions.

Photo: Trung Vo Chi

Are mobile phones secure enough for financial services?

CGAP

Mobile phone security

Mobile phones enable customers to access DFS. They are an important element in ensuring the security and confidentiality of customers' accounts. It is vital that:

- Hackers cannot access phones to see what is stored on them.
- DFS data and transactions, including PINs, cannot be eavesdropped.

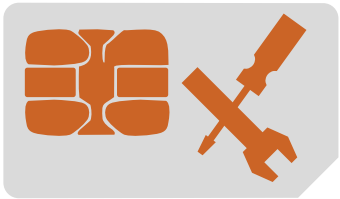
Properly securing mobile phones requires action not only from DFS providers, but from phone manufacturers and customers, who should be made aware of their responsibilities.

Feature phones

Feature phones are the most affordable mobile phone option. They remain dominant in low-income countries and among poor populations.

They do not contain much sensitive information and cannot be manipulated remotely, so there is not much of an incentive to hack them.

However, feature phones lack encryption, so they cannot protect against lack of security in the mobile network.



Use of a properly designed **SIM Toolkit app** can help address the security gap; an alternative is enhanced transaction monitoring by the DFS provider.

CGAP

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. Some are better than others in this regard. Many do not provide security updates once the phone is more than two years old.
- **Smartphone owners** should update their phone's software as soon as a new version is available. Some smartphone owners remove security controls (i.e., "rooting" or "jailbreaking") because they do not like the constraints they impose. Sometimes they do not understand the security implications.

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

CGAP

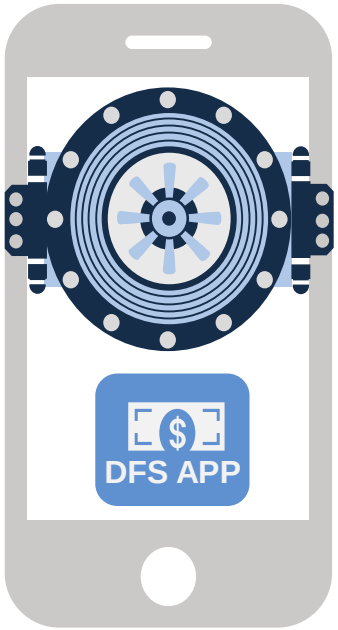
How to make phones more secure

Ideally, DFS applications should operate in a **secure execution environment (SEE).** An SEE is an electronic version of a bank vault. It is a secure place to keep customers' money. Every mobile phone, including feature phones, has at least one SEE: the SIM. But access to the SIM is controlled by the MNO.

Smartphone manufacturers can (and do) build their own SEEs into phones. But it is complex for DFS providers to access these SEEs, with multiple issues relating to handset ownership and cryptographic key distribution. Consequently, these SEEs are typically used only by the manufacturer (e.g., "Apple Pay", "Samsung Pay", etc.)

This means SEEs are not available to DFS providers, so they must look elsewhere to secure their apps.

SEEs are a great idea, but for commercial and technical reasons they are not available for use by DFS providers.



CGAP

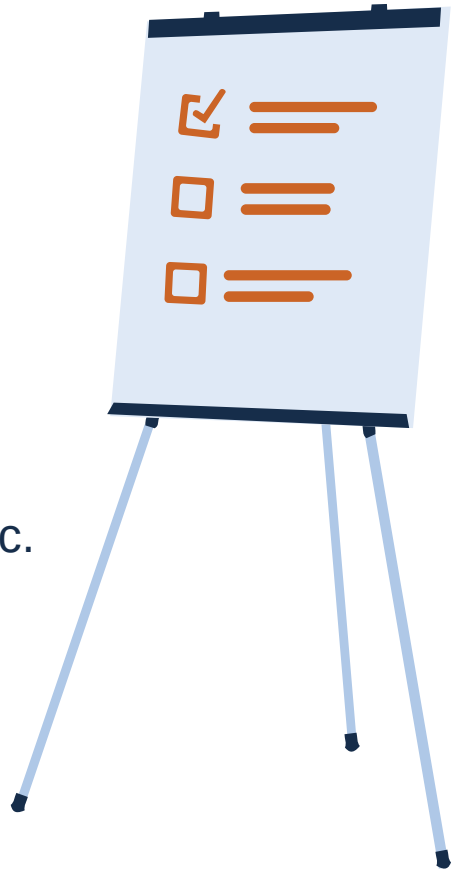
How to make phones more secure

DFS customers should:

- Make sure other people can't use their phones, by using a PIN or a biometric to control access.
- Install updates as soon as they become available.

DFS providers should:

- Provide a suitably secured app and not offer services through a device's browser, if possible.
- Control access to the app by using a PIN or a biometric. (This also applies to **feature phones**, where access is via USSD or via an app hosted on the SIM Toolkit.)
- Update the app to address any security shortcomings as they are discovered, and push updates out to customers.



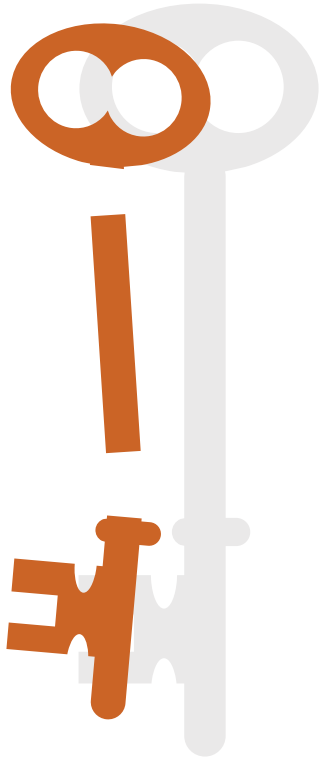
When payments are embedded within another app through an application programming interface (API), the embedded payment app must continue to manage its own security, as is the case with any API-led payments service.

CGAP

How to make phones more secure

DFS smartphone app developers should find other means of protecting their services and their customers:

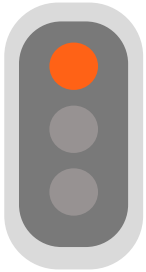
- Encrypt the app.
- Break up the app's cryptographic keys into small parts and hide them around the app, rebuilding only when needed.
- Obfuscate (hide) the purpose of data used, using suitable development tools.
- Develop the app to operate in smartphone's sandbox, where available (i.e., a technological sandbox, not a regulatory sandbox).



Are app-based transactions more secure than USSD- or SMS-based transactions?

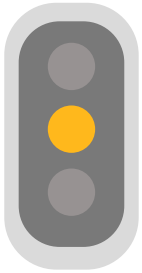
CGAP

App-based transactions have fewer vulnerabilities



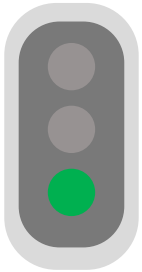
USSD has major security vulnerabilities:

- No security from customer's handset right through to MNO's back office systems, allowing hackers to eavesdrop account details and PINs.
- A hacker can push a USSD session to the customer in a way that looks like the DFS provider is contacting them. They can ask the customer to change their PIN, which can then be captured.
- Never more secure than using an app.



SMS is little better:

- Like USSD, it is unencrypted.
- Using SMS for "two-factor authentication" is bad practice because SMS can be snatched out of the air by a hacker misusing the roaming service.
- Old SMS messages are stored on the handset for people to read.
- ***The sole exception is the use of SIM Toolkit Apps that do their own encryption of SMS.***

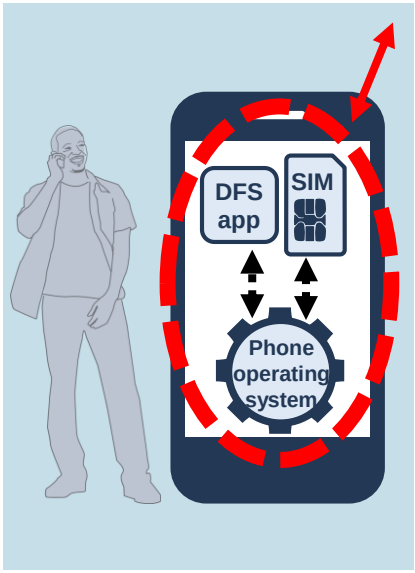


Smartphone apps are the best option:

- Smartphones support well-understood techniques to enhance app security.
- However, most of the lower-income and un(der)banked do not use apps.

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

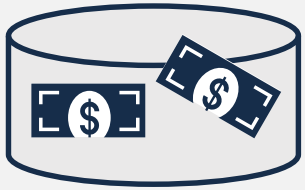
Best practice is to provide their own end-to-end security or, where this is not possible, follow alternative approaches.



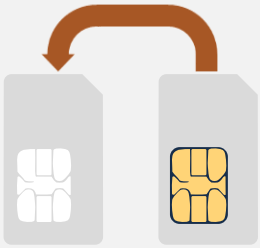
SIM swap fraud is a major problem for USSD and SMS

A SIM swap is the transfer of a mobile phone number from its original SIM to a new SIM. It is an important service that allows customers to keep their number and account after acquiring a new SIM card (e.g., because the old one got lost or they switched providers), but it is often misused to defraud DFS agents and customers. In fact, it is the most common risk for USSD- and SMS-based DFS. It does not apply to app-based services (including SIM Toolkit).

The victim's phone dies when their SIM is swapped to another controlled by criminals.



The criminals then transfer the victim's money to themselves and their associates.



The SIM is swapped back to the victim, whose phone comes back to life with an empty wallet.

SIM swaps are particularly problematic if the DFS provider is not an MNO, as these providers often have a limited understanding of mobile network technology.

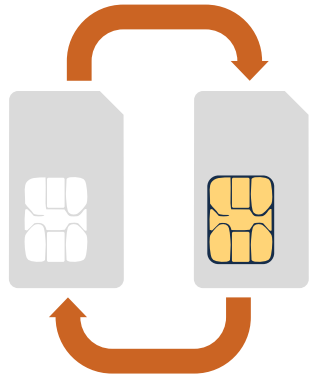
SIM swaps often follow eavesdropping attacks, in which criminals capture DFS customers' login credentials. The SIM swaps allow the criminals to hijack customers' accounts using the stolen PINs.

CGAP

SIM swap fraud can be counteracted

SIM swap fraud can be prevented through simple controls:

- Swaps should be disabled for SIMs that belong to prominent individuals or that are part of the DFS service (SIMs of agents and employees), unless senior management approval is obtained.
- Multiple SIM swaps within a short period should be disabled.
- Every DFS provider that is not an MNO should foster a good relationship with all of the MNOs in their country, not least in order to restrict and monitor SIM swaps.



CGAP

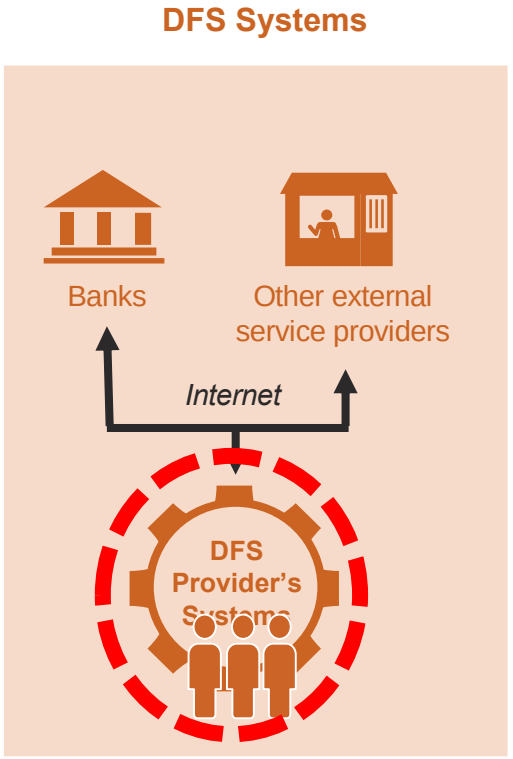
How can DFS providers secure their systems and transactions?

CGAP

Focus on insider threats first

Although hacking attacks and fraud perpetrated by agents generate the most media coverage, the **most successful attacks in terms of the total value of money defrauded are insider jobs** by DFS provider staff.

DFS providers' cybersecurity efforts should **focus on insider threats first.** Otherwise, they risk financial loss, loss of customer confidence, and potentially bankruptcy.



How to mitigate insider threats

Tip 1: Know your staff

Cybersecurity can be undermined by malicious staff. DFS providers should conduct appropriate background checks when recruiting staff. Checks should include:

- Police or criminal records
- Credit reference checks to identify excessive debt

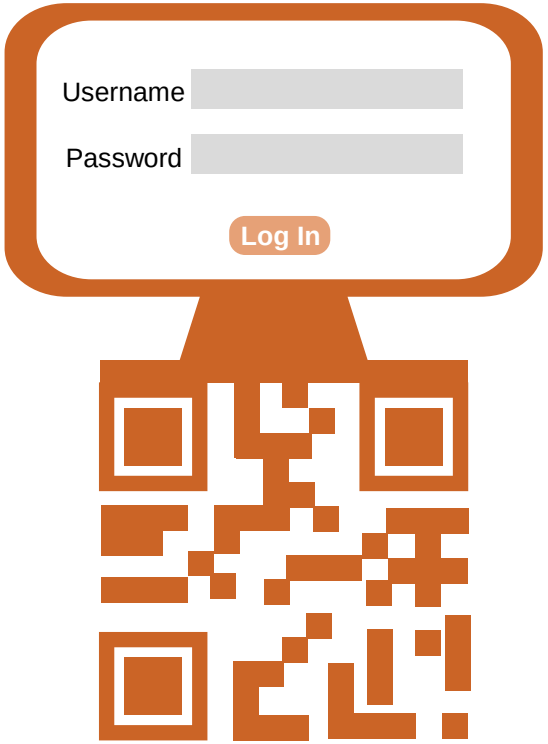
Background checks should apply to all senior staff and any staff involved in:

- Accessing or configuring the DFS platform
- Financial activities
- Customer-facing roles

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:

- Require staff to login using a username and password along with an additional factor, such as a scannable QR code.
- Do not use SMS-based methods.
- Staff in sensitive positions should use a key fob that generates temporary passcodes.

Logging of logins:

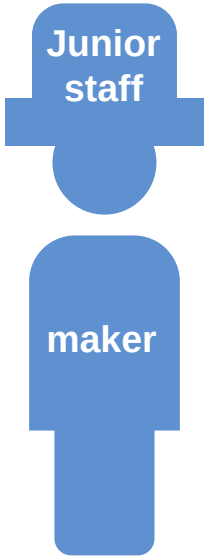
- Record all login attempts, successful or not.

CGAP

How to mitigate insider threats

Tip 3: Role-based access and auditability

Money transfer functions should be carefully controlled through:



- **Role-based access.** Someone whose job does not involve money transfers cannot access the functionality.
- **Maker/checker controls.** A junior staff member can make, but not check or approve, transfers. A manager cannot make, but can check/approve, transfers.

These controls should be reinforced by recording logins and by making investigation and auditing tools available to senior management.

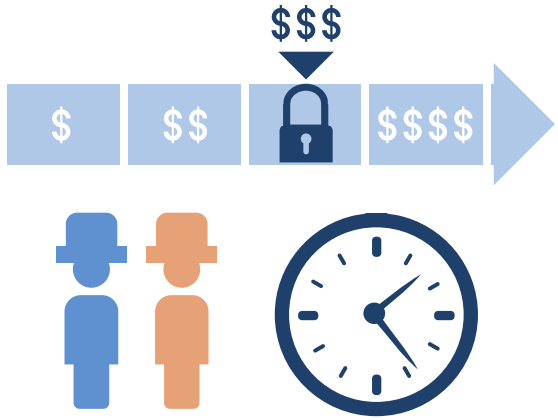
How to mitigate insider threats

Tip 4: Processes and control points

Carefully defined and implemented business processes not only improve a business's operations, they mitigate staff error, over-reliance on key staff, and lack of knowledge sharing.

Processes are best developed and operated using a **business process management service**. They should include a set of **control points**, such as:

- Transaction value beyond which additional authorization is required
- Particular person that is required to carry out a function
- Time of day when a function may only be performed (e.g., during office hours)



CGAP

How to mitigate insider threats

Tip 5: Regular reconciliation of accounts

Making sure recorded transactions, the values in customers' accounts, and the overall value in the bank accounts are in agreement is crucial to maintaining the financial integrity of a DFS service. Many well-known insider jobs could have been detected earlier through rigorous reconciliation and reporting.

Reconciliation has two main functions:

- Ensure all customer balances are secured by real funds in a bank account.

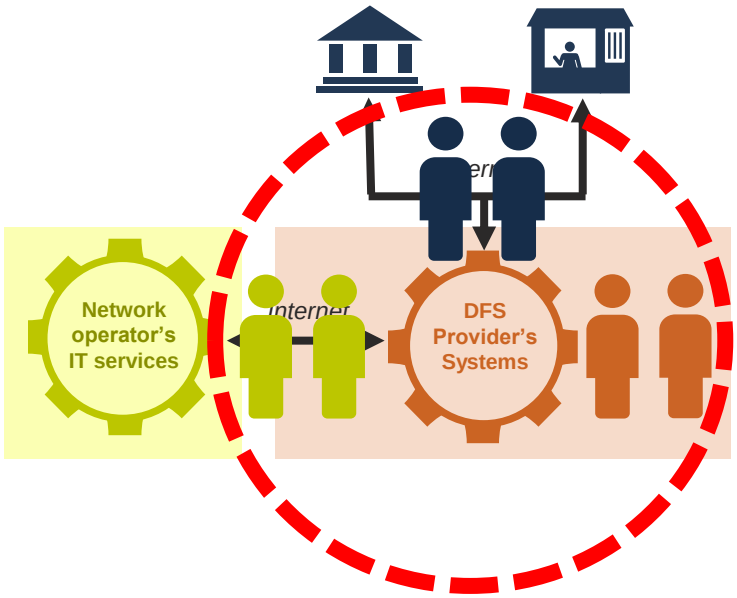
- Indicate potential fraud perpetrated by breaching cybersecurity controls and controls for the creation of value.

Adopt measures to protect against third-party threats

Once a DFS achieves a degree of success, it will **attract the attention of external hackers**. Attacking the service directly offers potentially greater rewards than attacking agents or customers.

The most effective means of doing this involve **electronic attacks** (hacking into networks and systems via the internet) or **physically accessing** the service by visiting the provider's site.

Protections against all the various means of attack must be in place.



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, which might, for example, make them subject to coercion to provide improper access to DFS providers' information.

This vetting process should be a regular part of annual due diligence. It also requires a common understanding of the division of responsibilities and liabilities in case of fraud.

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 among:

- A DFS provider and its customers, suppliers, and other external parties
- A DFS provider's staff and inter-process systems

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 active, automated transaction monitoring and alert functions.

Appoint a fraud officer to monitor transactions, submit suspicious transaction reports, and support further investigations.

Transaction investigation tools with ”follow the money” functionality can be leveraged for rapid investigation of potential crimes.

In addition to the detection and prevention of fraud, active, automated transaction monitoring can contribute to a DFS provider’s anti-money laundering/combatting the financing of terrorism (AML/CFT) compliance obligations.

CGAP

How to mitigate insider and third-party threats

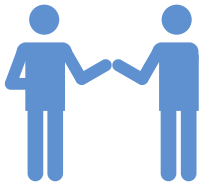
Tip 4: Physical security

Physical security is the first step in ensuring cybersecurity and limits the opportunity for the subversion of cyber-controls. Well-managed data centers **focus equally on physical and cybersecurity**. At a minimum, physical security involves:

- There is only one, strictly controlled entrance to DFS providers' premises.
- Other entrances are secured, and fire exits have alarms.
- All rooms are secured with biometric locks, require touch in and touch out to avoid tailgating, and access is restricted based on job function.
- Staff in customer-facing roles or in the finance department are not allowed to have their mobile phones with them on the premises; phones should be stored in metal lockers during working hours.
- Video surveillance and 24-hour recording of all areas (cameras must face away from screens that might show sensitive information).

How to mitigate insider and third-party threats

Tip 4: Physical security (Cont.)



Physical security measures also apply to visitors:

- Check and log visitors' identities.
- Do not permit visitors to bring **any** electronic equipment into operational areas.
- In **non-operational areas only**, mobile phones and laptops may be allowed. However, the serial numbers of laptops should be logged, and providers should check to ensure visitors leave with the same equipment they brought. Switching laptops is the fastest method of stealing data.
- Ensure visitors are accompanied by a staff member who is responsible for their conduct.
- Continually remain aware of visitors' activity:
  - Do not let visitors wander unaccompanied.
  - Do not let visitors insert USB drives or other devices into company laptops, printers, etc.

How to mitigate insider and third-party threats

Tip 5: Cybersecurity reviews

Every DFS service should undergo an external cybersecurity review before launch and at regular (annual) intervals after launch. Findings, including the vulnerabilities identified and recommended countermeasures, should then be presented to the DFS provider's senior management team.

Supervisors should require DFS providers to undergo these external cybersecurity reviews, to report the final results and their action plans to supervisors, and to implement effective and efficient countermeasures in a timely manner.

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:

- Using a properly-secured smartphone app
- Encrypted SMS, using a SIM Toolkit app hosted on the SIM, works for both feature phones and smartphones

In most lower-income countries, this is not possible because of:

- Low smartphone penetration
- The DFS provider may not be able to place an app on customer SIMs

Therefore, any DFS provider must implement and use sophisticated monitoring processes and facilities in order to counter fraud.

Due to the additional risk incurred by using USSD, when assessing a service that relies on this technology, **supervisors** should place particular emphasis on the quality, availability and continuous use of such essential monitoring facilities by DFS providers.

Create an expert body to issue and update security standards

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

Technical standards need to be set, but they must also be dynamic to reflect:

- Continual evolution of best practices
- Emergence of new threats
- Recent technologies and protocols
- New approaches to mitigation

Instead of technical standards, regulators should specify:

- An expert body that issues security standards (such as a national or regional cybersecurity authority or NIST's Information Technology Laboratory)
- Requirements to conform to this body's security standards
- An inspection/audit regime
- A mechanism for responding to new threats

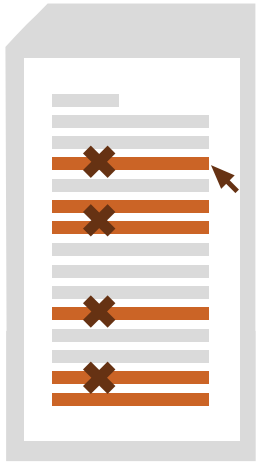
CGAP

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. Issues to consider include:

- Mandatory communication to the authority and affected customers
- Requirements to refund the losses from customers' accounts
- Potential liabilities for customers' consequent losses



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

For example, regulators can require a customer complaint about fraudulent activity in their account to result in immediate refund (into escrow[1]; with escrowed payments being either returned or forwarded to the customer after investigation).

[1] In this context, an escrowed payment is held in an account under the control of a trusted third party (not the DFS provider); at the end of an investigation, the trusted third party will release the money, either to the customer or to the DFS provider.

CGAP

Consider responsibility 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.

CGAP

Recommendations

CGAP

Regulators

Regulators should:

- 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

Supervisory authorities should

- Engage DFS providers in a program of continuous improvement.
- **Adopt a comprehensive data security supervisory program**, including
  - Monitor DFS providers' compliance with the cybersecurity regulations.
  - Require annual cybersecurity review reports from DFS providers, review reports, issue notices requiring improvement where required, and monitor actions relating to those notices.

    → Such reviews should be carried out by qualified third parties, though this role may be undertaken by internal auditors as the capacity is developed.
  - Visit DFS providers' operational centers to verify that the process and control points that have been documented are being followed, and to verify that the active transaction monitoring (including AML monitoring) described in slide 37 is in place.
  - Review suspicious transaction reports (STRs) received from DFS providers, comparing them to those received from the rest of the financial sector, and act if they differ significantly in either expected numbers of reports, or the level of detail provided.

DFS providers

DFS providers should:

- Assess their exposure to risk and improve countermeasures where necessary.
- Annually engage a qualified third-party to carry out a risk assessment and cybersecurity review. Submit the 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, a DFS provider should give reasonable consideration to any identified security weaknesses and the consequent issues around fairness to customers.

Stay connected with CGAP

www.cgap.org

@CGAP

Facebook

LinkedIn

CGAP

CGAP

www.cgap.org