# Cybersecurity platform for financial sector by the Bank of Russia

Artem Sudarenko

BANK OF RUSSIA
FINCERT

# Cyber risk's factors

BANK OF RUSSIA
FINCERT

# Factors increasing cyber risk



Aforethought

Instrument

Ways to cash out

Villain

# Factors increasing cyber risk



**Aforethought**

**Villain**

**Instrument**


**Malware**


**Phishing sites**

**Skimming**

**Ways to cash out**

# Factors increasing cyber risk



## Aforethought

Villain

## Instrument


Malware


Phishing sites

Skimming

## Ways to cash out

# Factors increasing cyber risk



## Aforethought

Villain

## Instrument


Malware

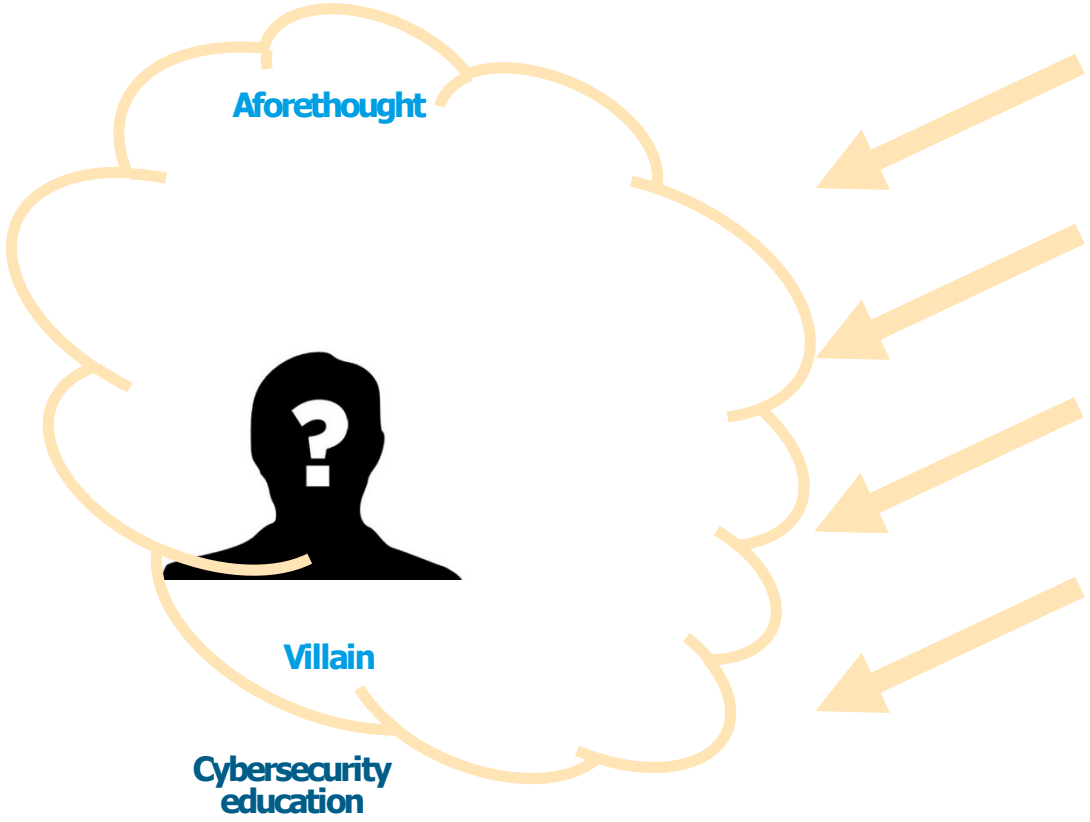

Phishing sites

Skimming

## Ways to cash out

# Factors decreasing cyber risk






## Users of financial services

## Pupils & Students

СИРИУС
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

# Factors decreasing cyber risk



**Exploring villain's technologies and sharing the results**

**Instrument**


Malware


Phishing sites

Skimming

**Ways to cash out**

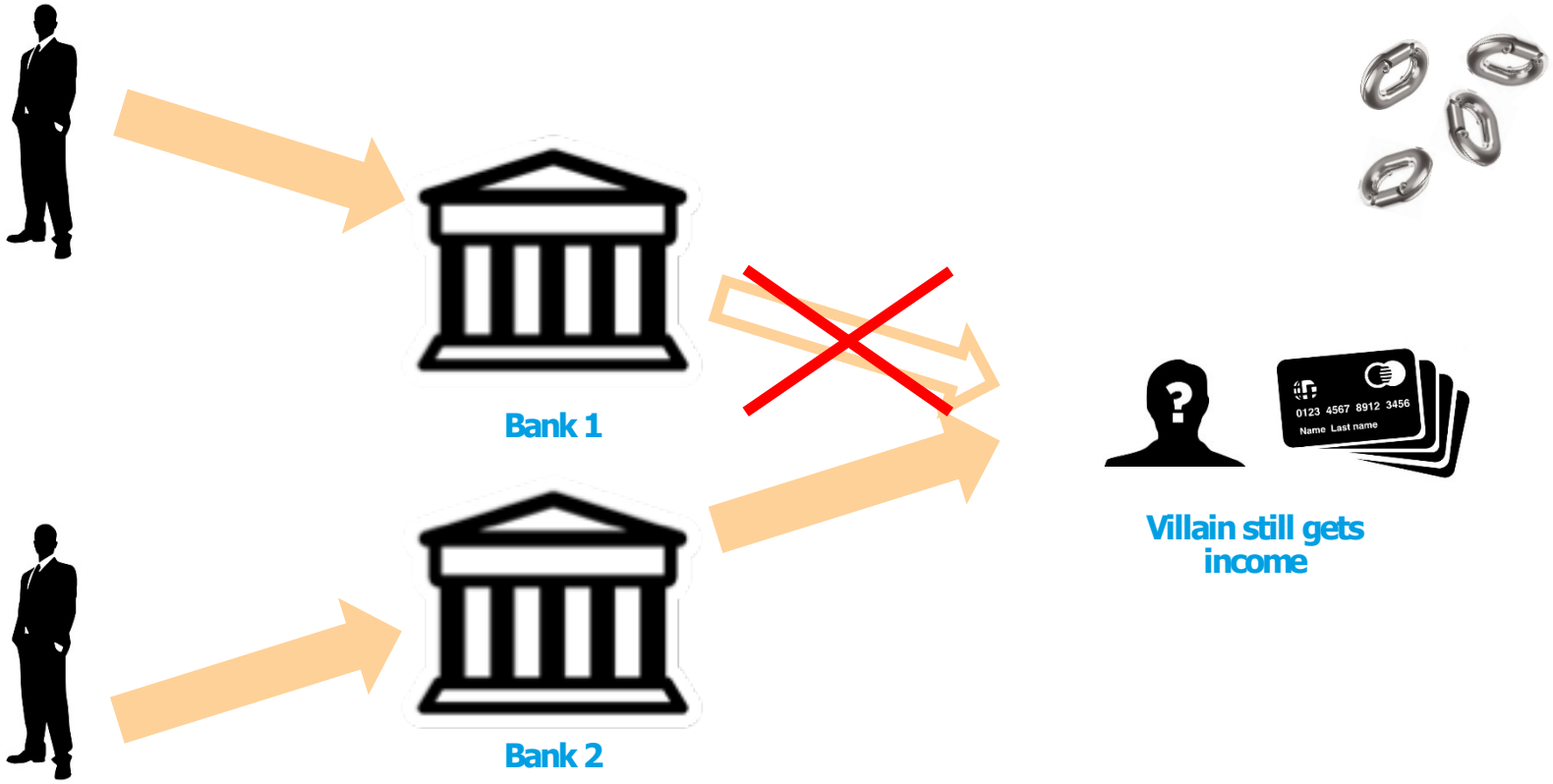
**Cybersecurity information exchange**

# Cybersecurity information exchange

BANK OF RUSSIA
FINCERT

# No cybersecurity information exchange





# The first goal – to integrate all banks into exchange



| | |
|---|---|
| Banks must get access to automated system for cybersecurity information exchange implemented by the Bank of Russia considering recommendations of the Bank of Russia (September 30 is the deadline for getting access) | ***Automated system for cybersecurity information exchange implemented by the Bank of Russia*** |
| Banks must notify the Bank of Russia about the existence of new problems and incidents associated with providing the data security for funds transfer (Article $2.13^{1}$ ) | ***Bylaws of the Bank of Russia (including amendments)*** |
| Banks must provide the data security for funds transfer considering regulatory acts of the Bank of Russia governing relations in the national payment system (Article 27) | ***A Federal Law on National Payment system (including amendments)*** |

As exchange is organized by Federal Law on National Payment system it is **free** for all its participates

# The first goal – to integrate all banks into exchange



**Chain only as strong as its weakest link**

**The second goal – to make information in exchange accessible by all participates**

# The second goal — to make information in exchange accessible by all participates

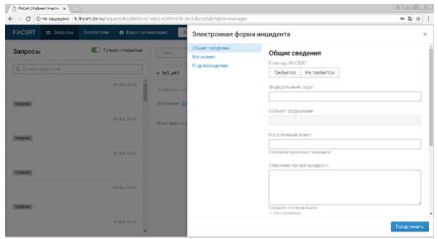


Manual

JSON

API (by the end of 2018)

Automatic




Incoming information

# The second goal — to make information in exchange accessible by all participates

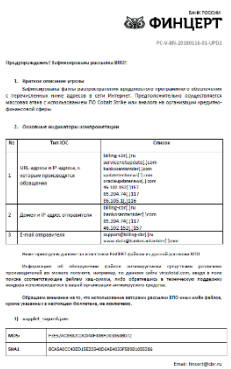


Manual

Machine readable (by 20 July)

API (by the end of 2018)

Automatic

Outgoing information is anonymized

# The second goal – to make information in exchange accessible by all participates

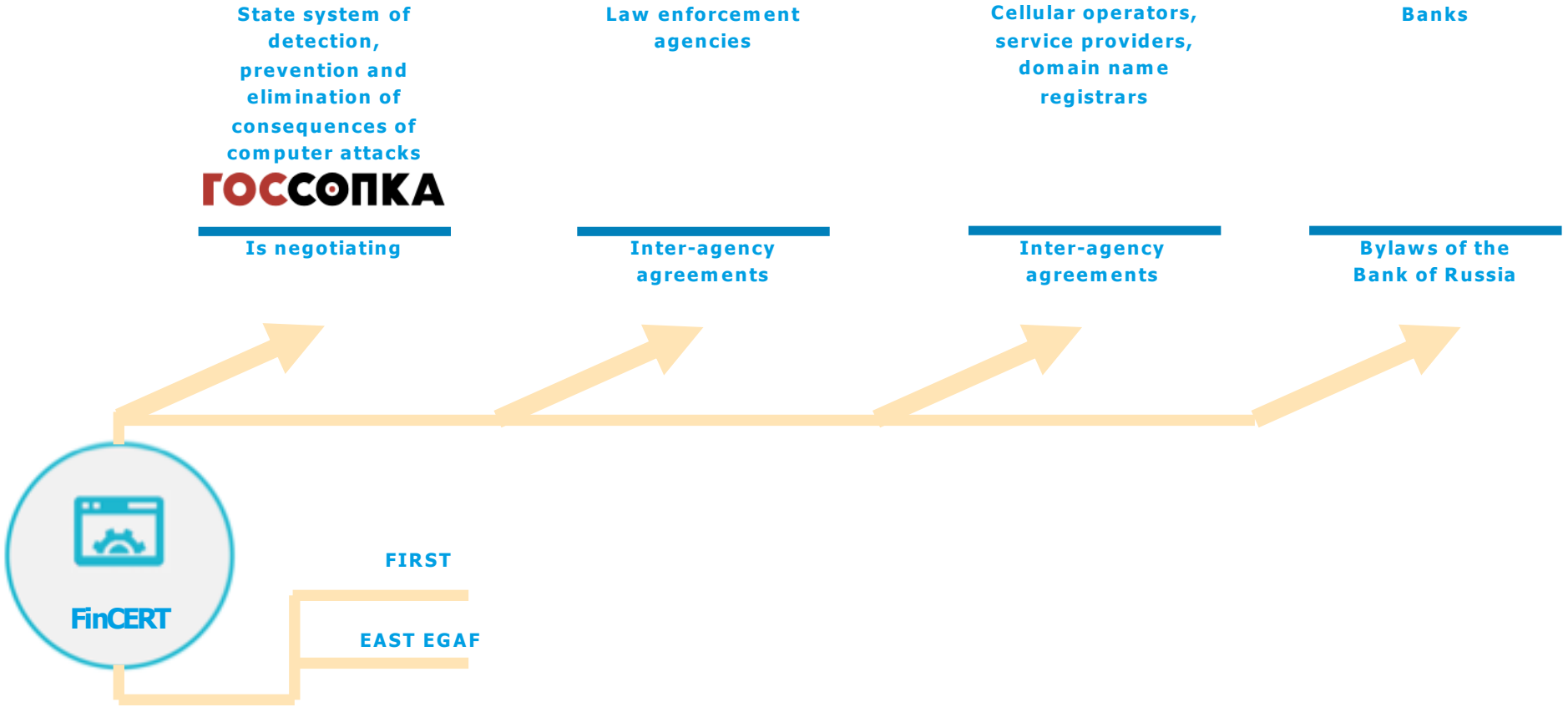


**Knowledge without application is useless**

**The third goal – to make information applicable**

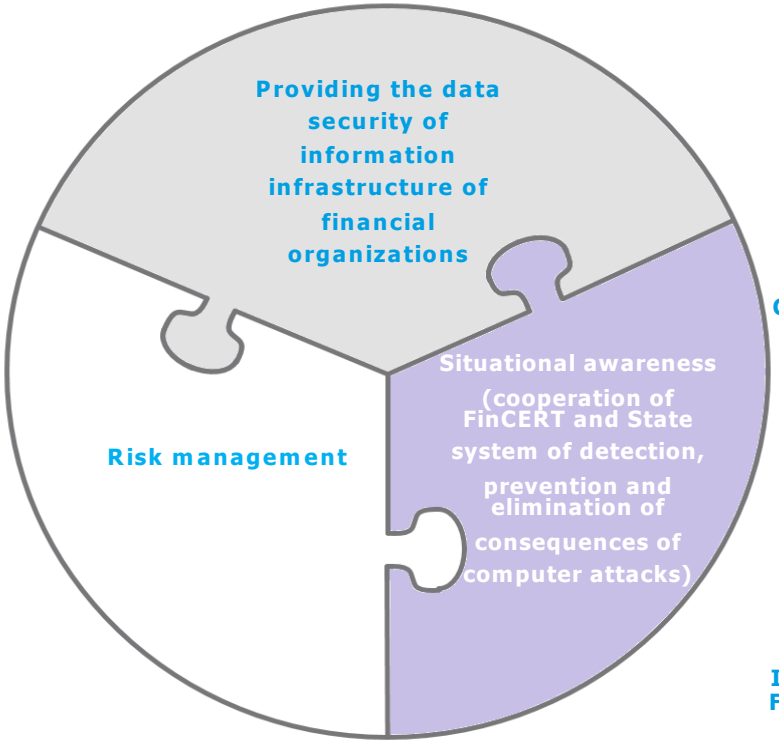
# The third goal – to make information applicable





# Reaching the goals. Structure of information exchange






Critical information infrastructure objects of financial sector – systems and networks operating within financial sector

A Federal Law on Security of Critical information infrastructure in the Russian Federation

State system of detection, prevention and elimination of consequences of computer attacks

ГОССОПКА

BANK OF RUSSIA FINCERT

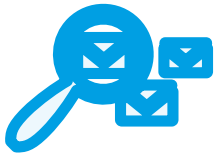
According to Doctrine of Information Security of the Russian Federation the Bank of Russia is the part of institutional framework of the information security system

Financial organizations

Format of data exchange is set in standard provided by the Bank of Russia. The standard is agreed upon with financial organizations and Federal Security Service of the Russian Federation

# Cybersecurity information exchange nowadays





## Blocking domains

**More than 1650 domains with fraudulent content blocked in 2017-2018 (especially connected with banking, insurance, FIFA world cup and funds transfers)**

**Number of information exchange participates:**

**430 – Banks**

**105 – Financial organizations (non-banks)**

**3 – Banking software developers**

**18 – Credit organization (non-banks)**

**7 - Cellular operators, service providers**

**3 – Antimalware software developers**

**3 - Law enforcement agencies**

**54 - Others**

***According to official reporting total amount of fraudulent funds transfers***

Accounts of juridical persons

- In 2017 – 1,57 billion rubbles
- In 2016 – 1,9 billion rubbles
- In 2015 –3,8 billion rubbles

Payment cards

- In 2017 – 0,96 billion rubbles
- In 2016 – 1,08 billion rubbles
- In 2015 – 1,15 billion rubbles

**KPI: Proportion of fraudulent funds transfers with payment cards among the total funds transfers with payment cards less than 0,005%**

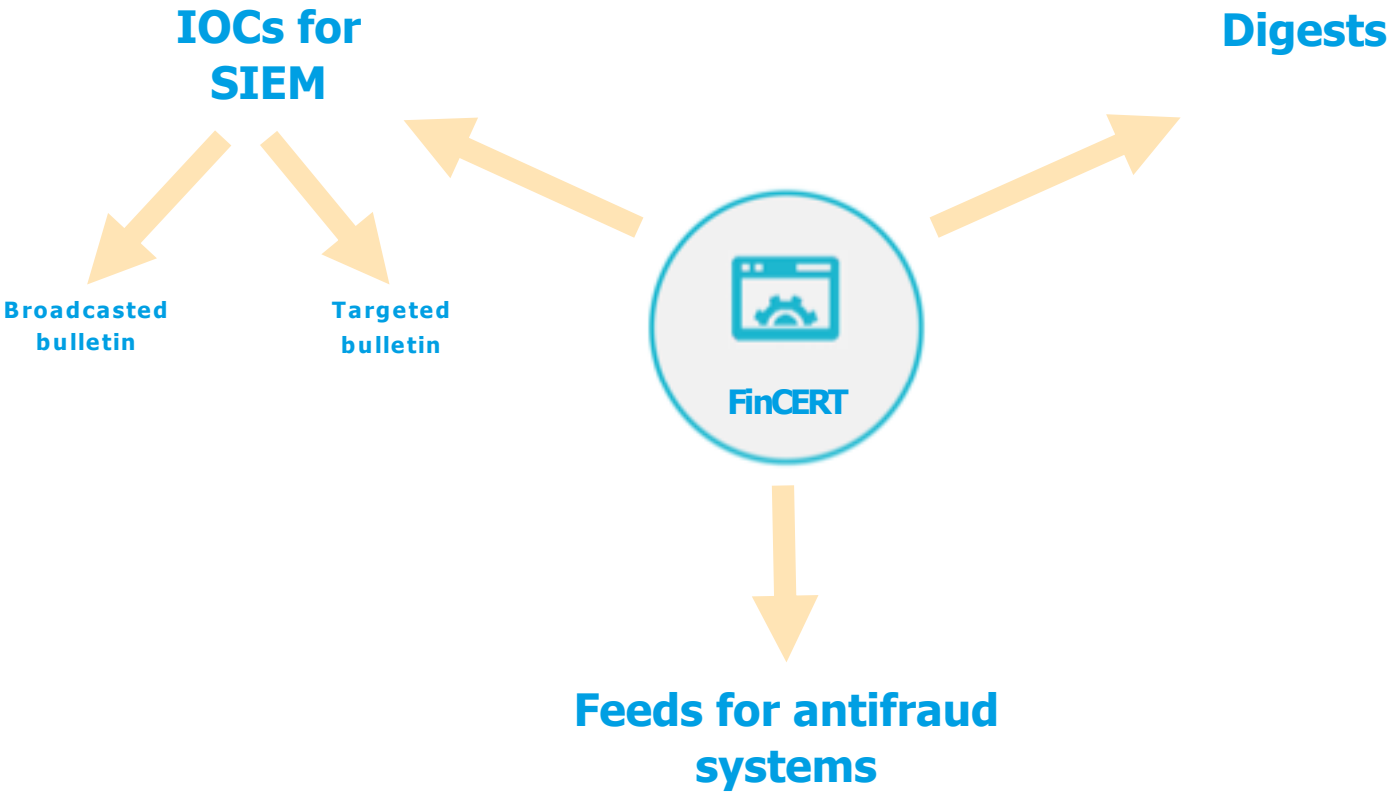
## Amount of bulletins

**Total: 402**

**In 2017: 119**

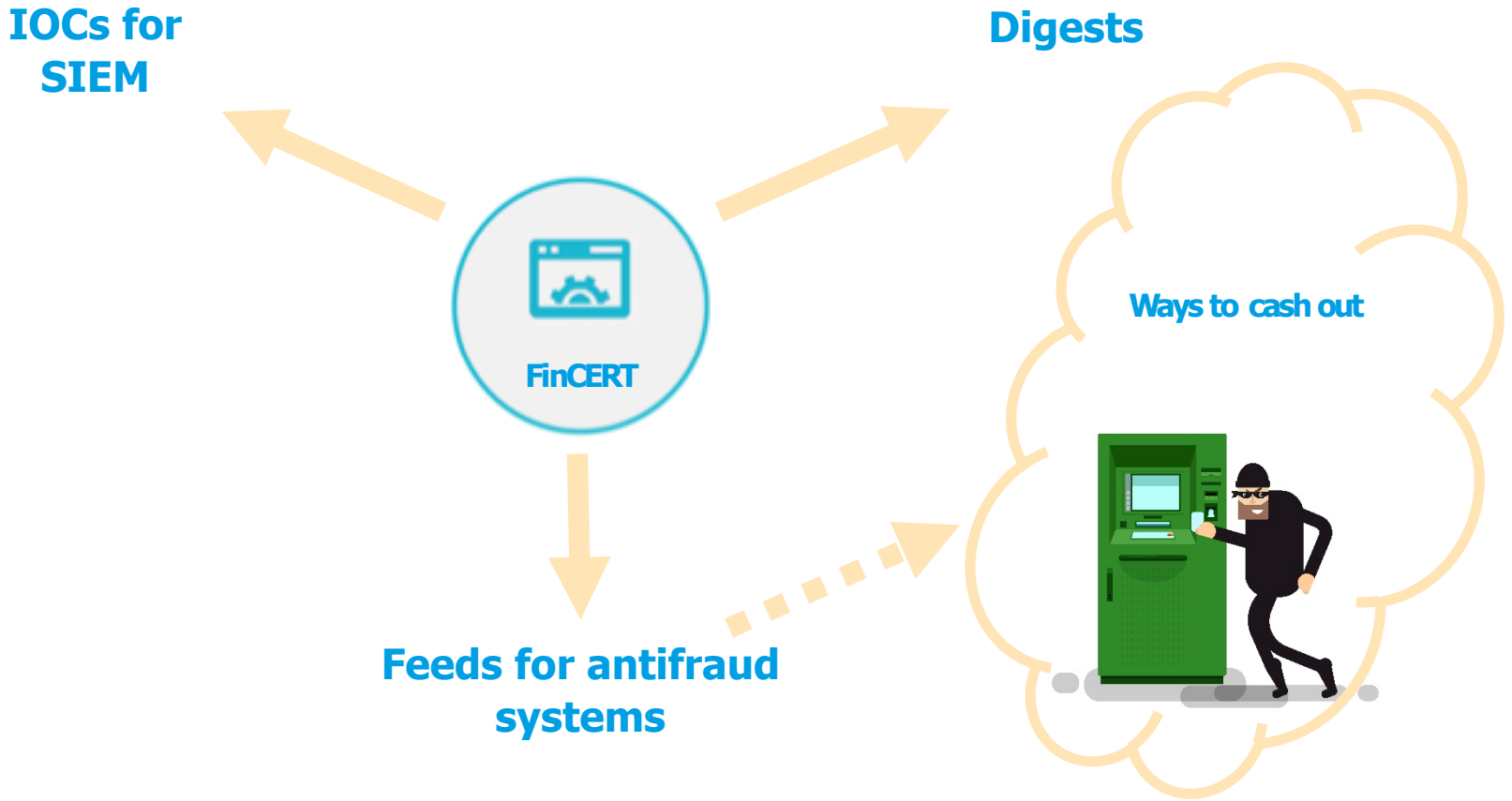
# Cybersecurity information exchange types of outgoing information





# Cybersecurity information exchange types of outgoing information





# Feeds for antifraud systems

BANK OF RUSSIA
FINCERT

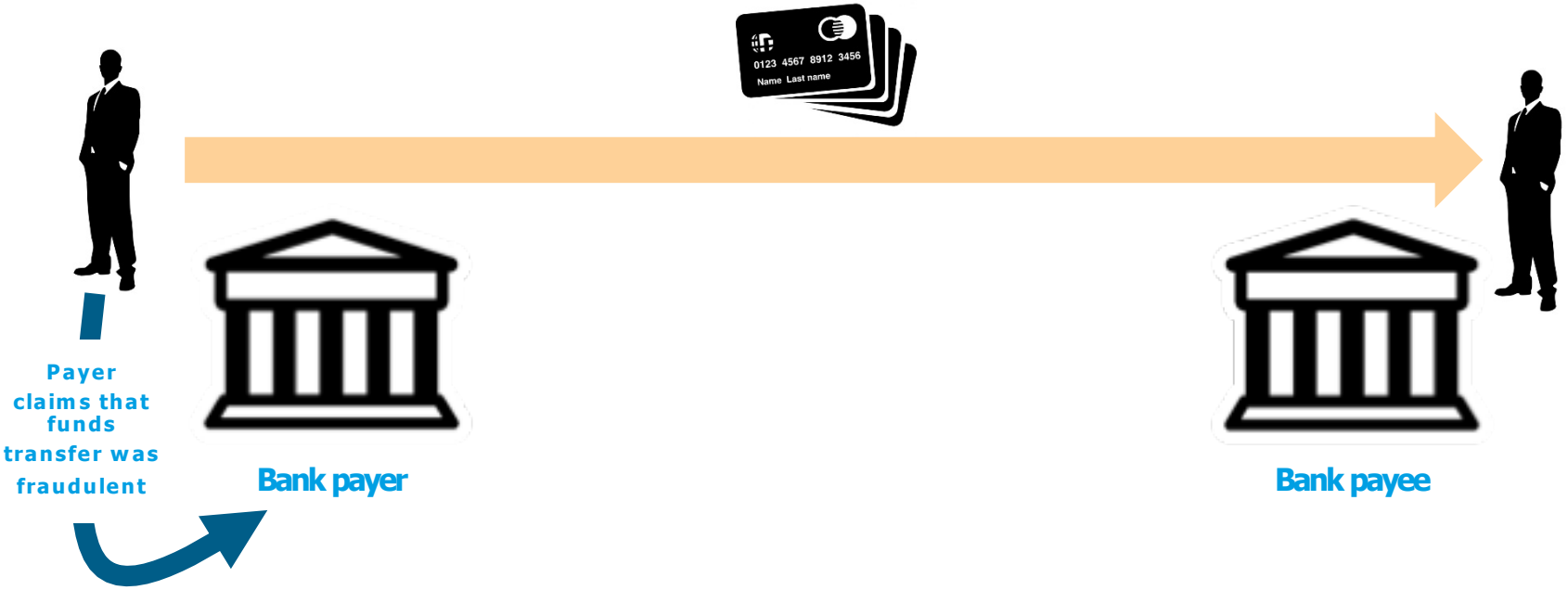
# The main goal – to raise bank's awareness of its customers




In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers






In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers




Payer claims that funds transfer was fraudulent

Bank payer

Bank payer reports to the Bank of Russia about fraudulent funds transfer

FinCERT

Bank payee

In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers




Payer claims that funds transfer was fraudulent

Bank payer

Bank payer reports to the Bank of Russia about fraudulent funds transfer

FinCERT

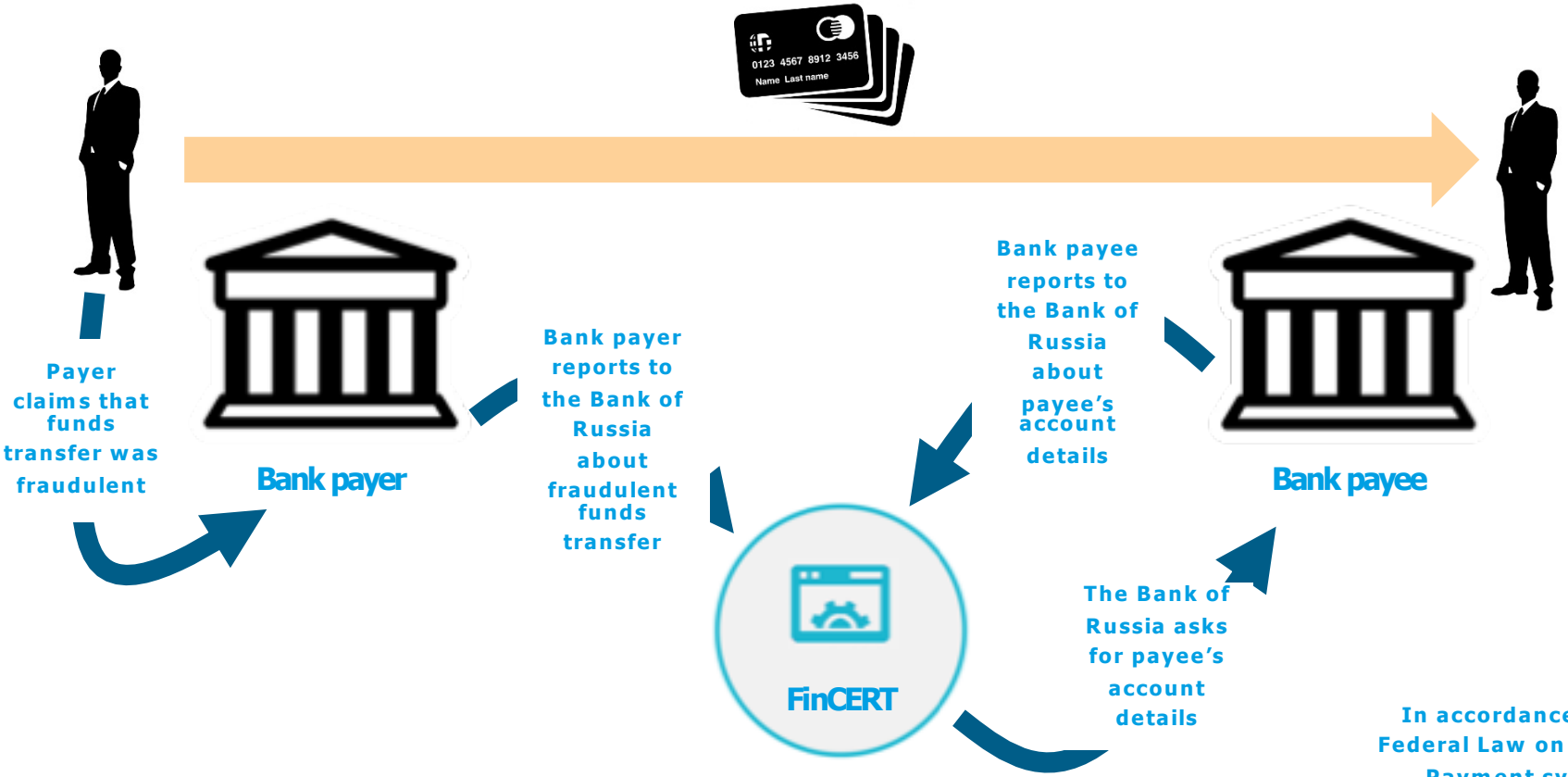
The Bank of Russia asks for payee's account details

Bank payee

In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers

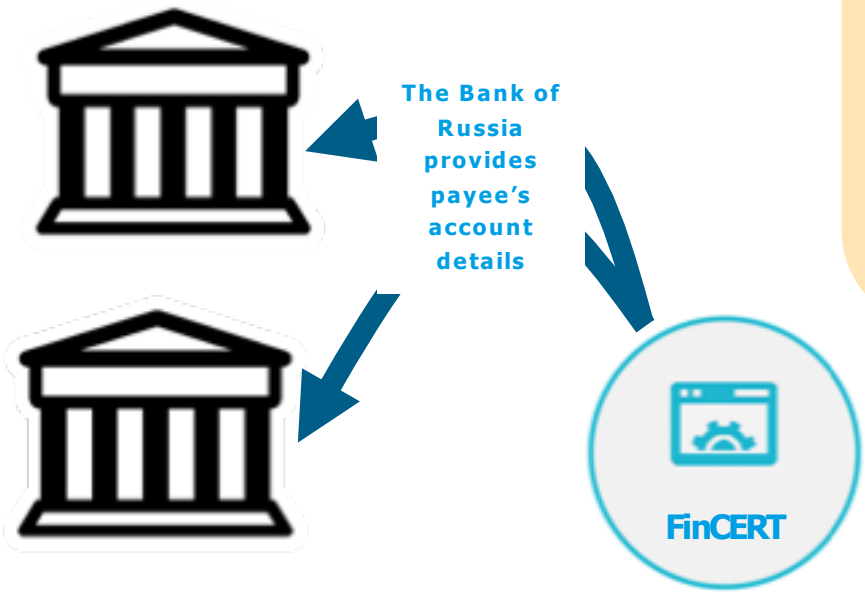





In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers



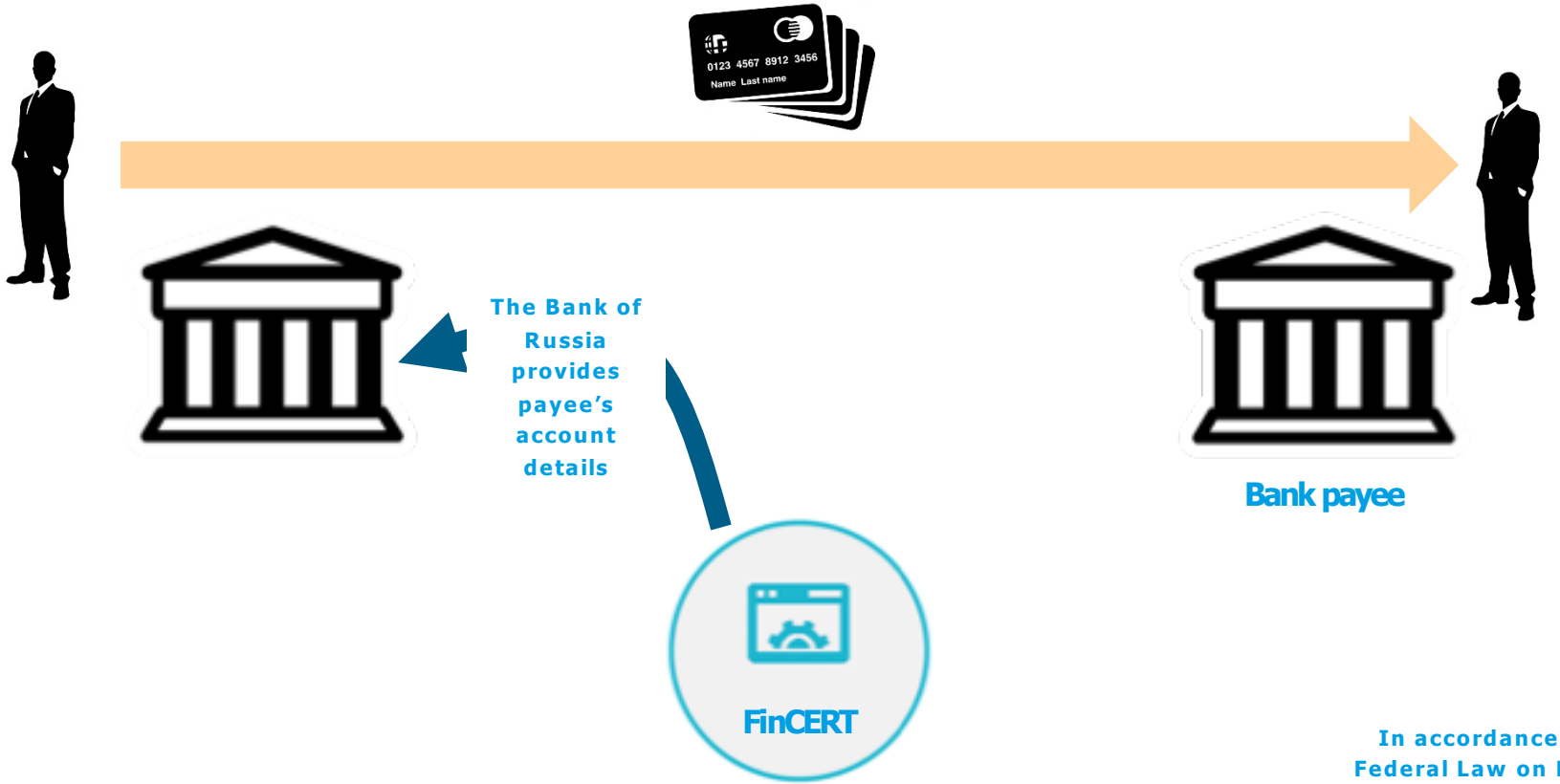



The Bank of Russia provides payee's account details because payee received a number of claimed funds transfer exceeded threshold value

In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers

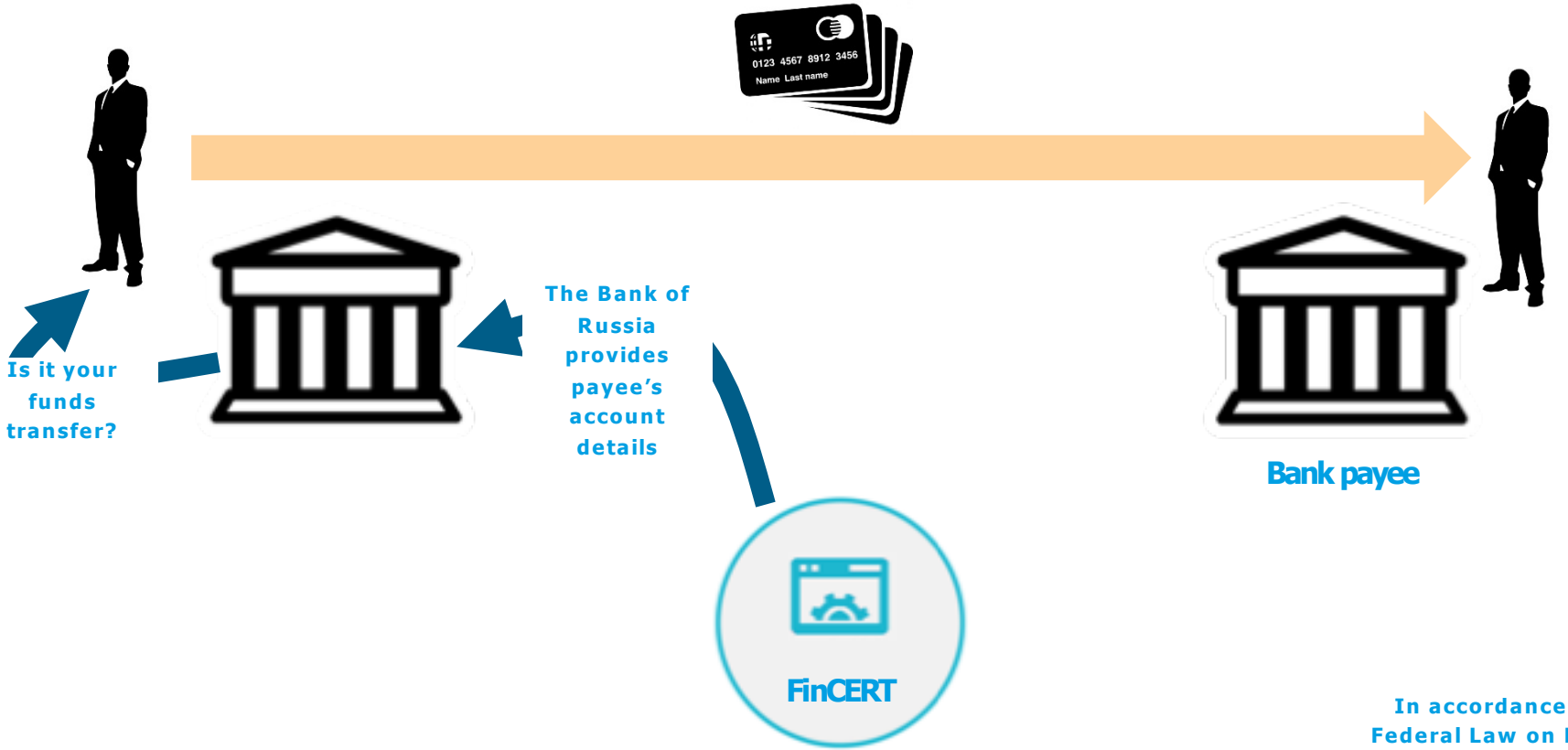





In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers

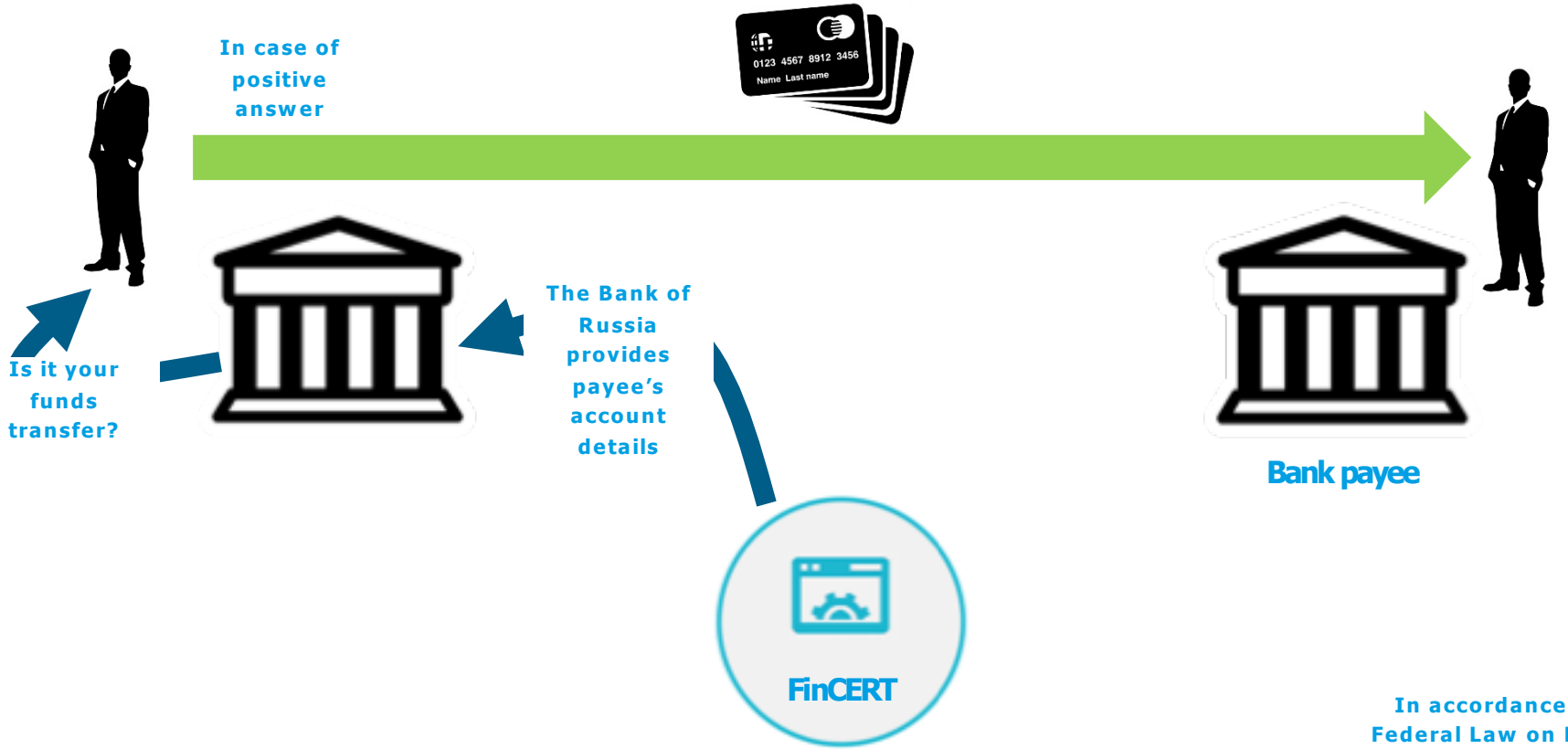





In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers

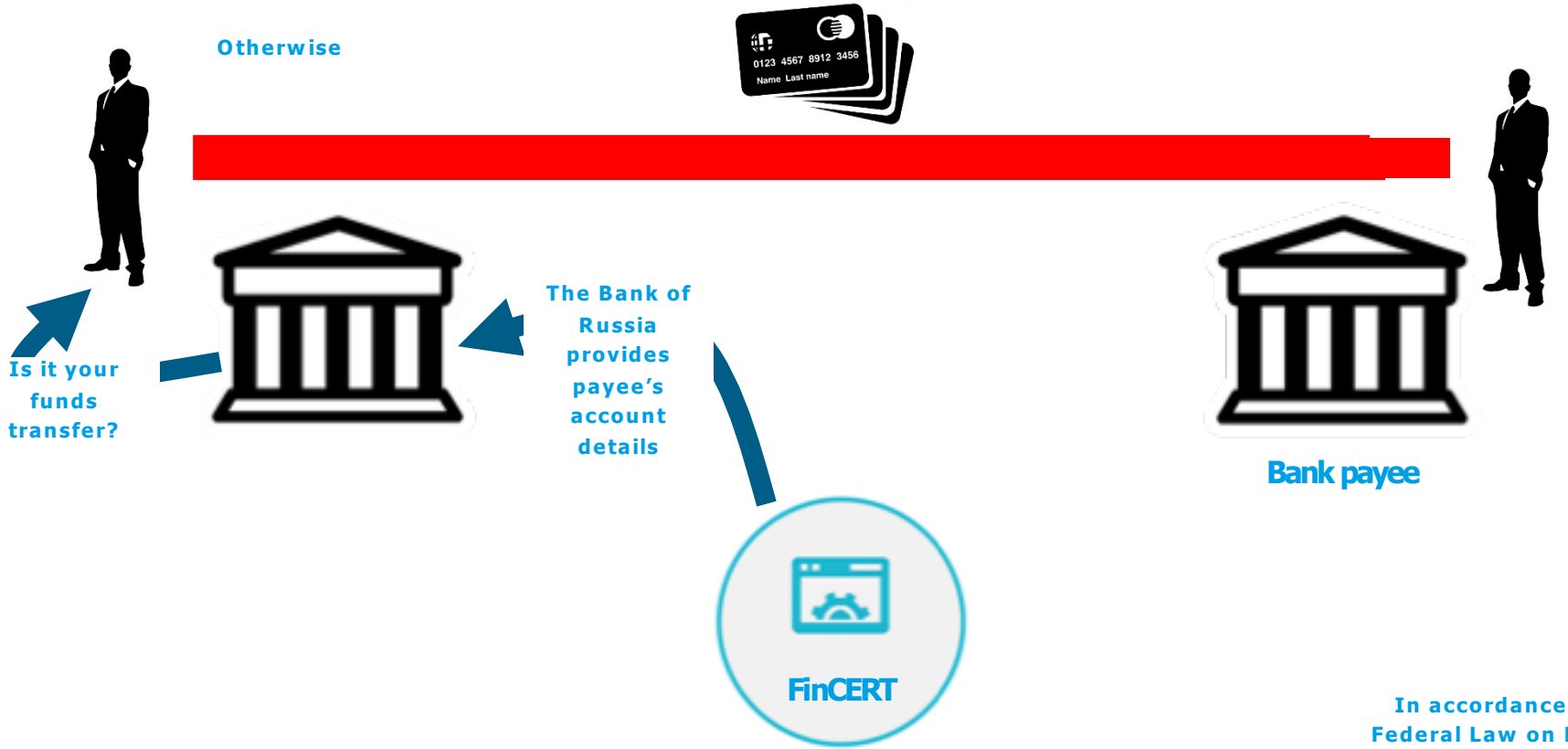





In accordance with a Federal Law on National Payment system

# The main goal – to raise bank's awareness of its customers





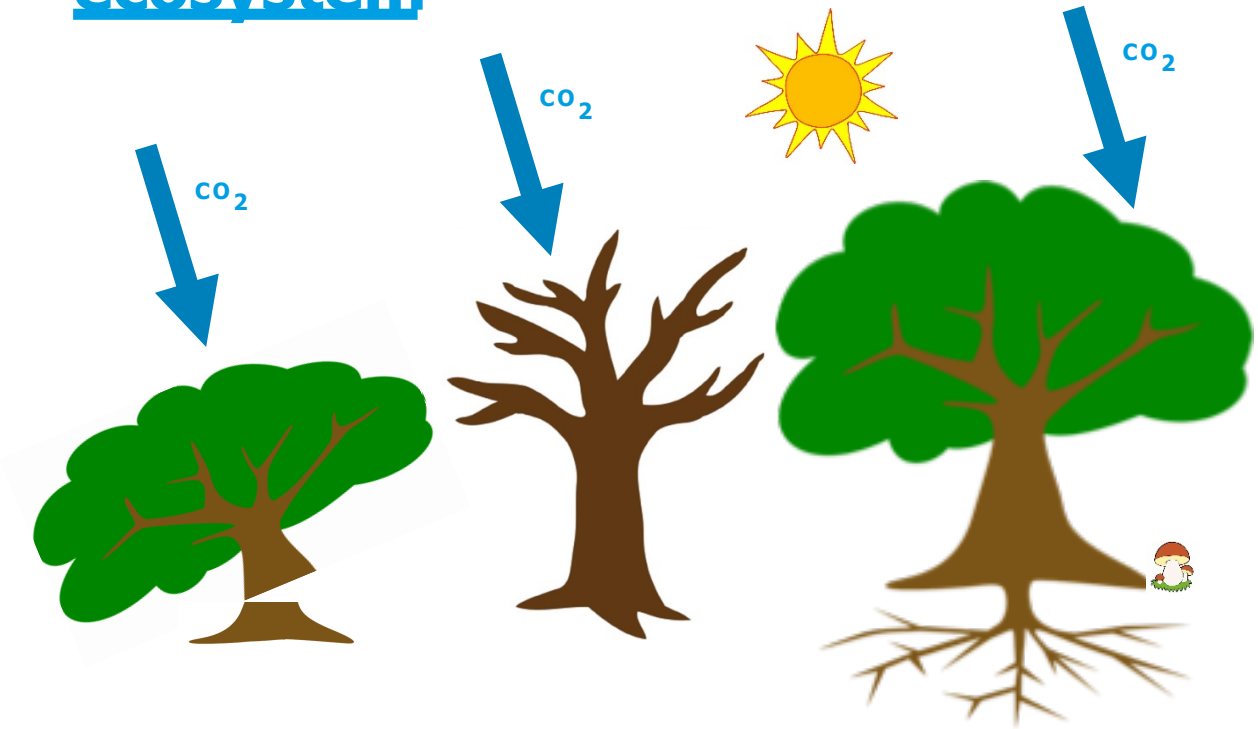

In accordance with a Federal Law on National Payment system

# In conclusion

BANK OF RUSSIA
FINCERT

# Cybersecurity platform for financial sector by the Bank of Russia is like an ecosystem






Federal laws and bylaws AS roots

Automated system for exchange AS leaves with chlorophyll

Incoming information AS carbon dioxide

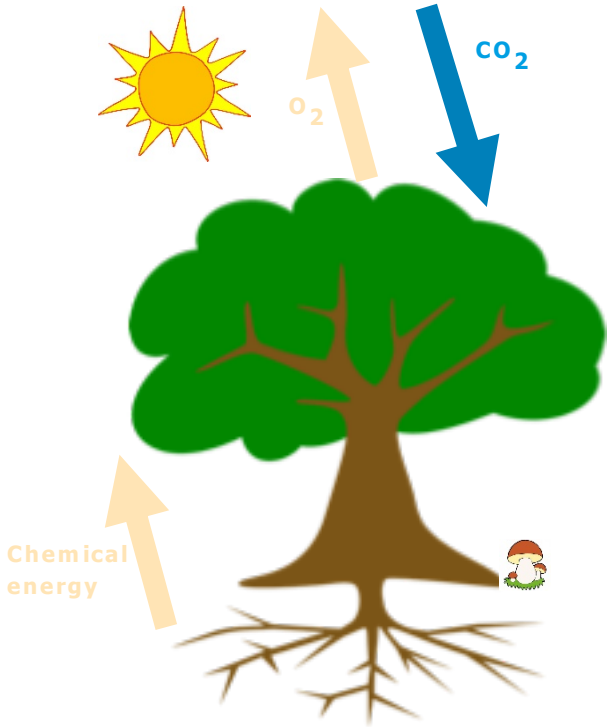
Team AS sunlight

Cybersecurity education and feedbacks AS symbiosis

# Cybersecurity platform for financial sector by the Bank of Russia is like an ecosystem



**Only healthy ecosystem can produce positive results**




Federal laws and bylaws AS roots

Automated system for exchange AS leaves with chlorophyll

Incoming information AS carbon dioxide

Team AS sunlight

Cybersecurity education and feedbacks AS symbiosis

Outgoing information AS oxygen and chemical energy

# Thank you for attention!

BANK OF RUSSIA
FINCERT