heksagon

PROTECT
INTERCONNECT
MONETIZE

Call Validation

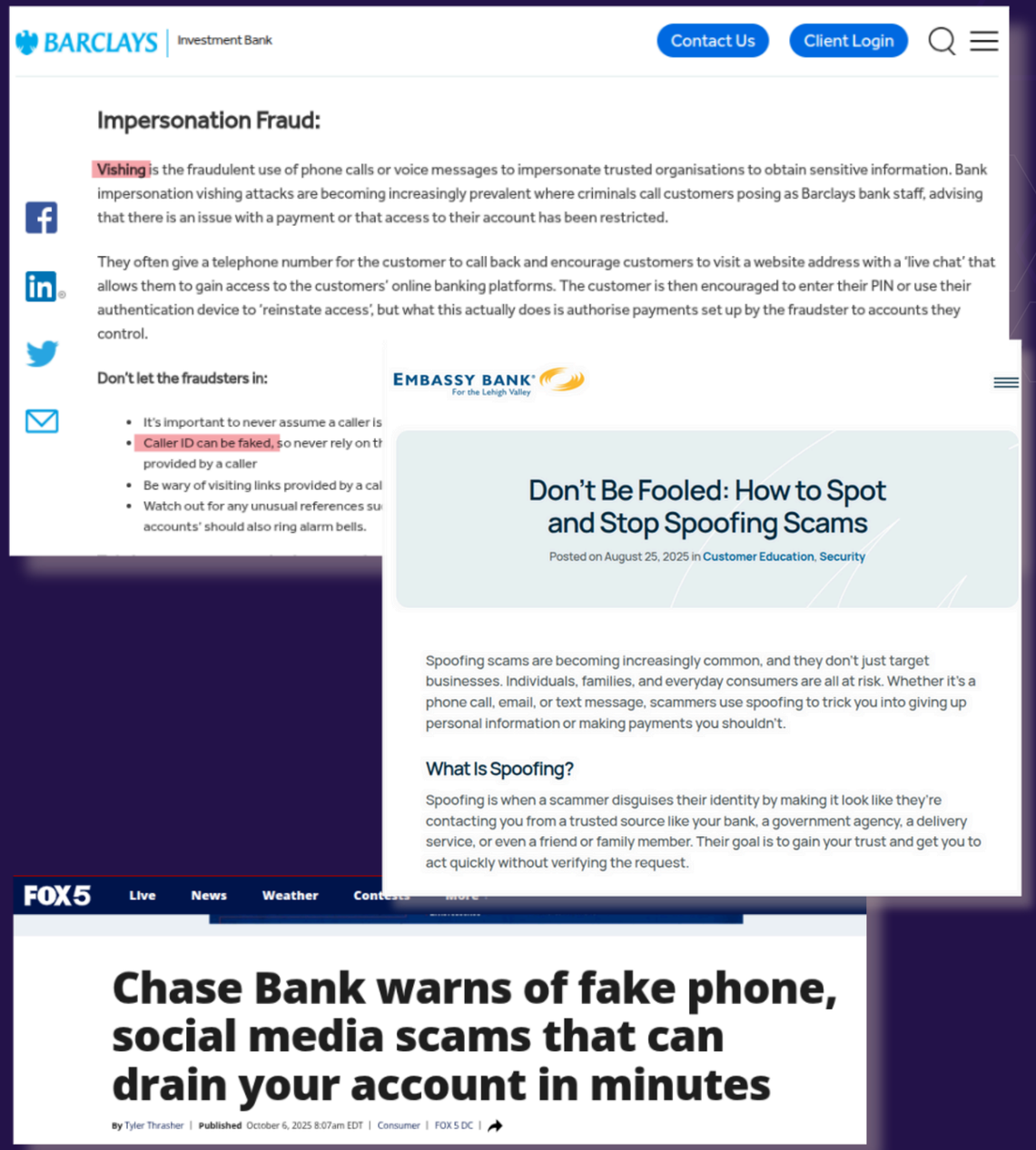
Help Banks Restore Trust in Every Call.

www.heksagon.com

CLI Spoofing Fraud

From a niche scam to a multi-billion-dollar vulnerability

- Several banks use mobile number CLI as key information to identify client in their call centers and follow simpler authentication procedure in case of known CLI.
- Likewise, bank clients often recognize bank phone numbers, UANs and trust such calls.
- There is a significant volume of Social Engineering fraud cases using the weakness of CLI spoofing to take advantage of this situation and obtain access to client bank accounts in such way.



Existing CLI Validation Challenges

Excessive Fraudulent Cases

Huge Revenue losses on part of customers and indirectly banks

Limited Capabilities

Banks and MNOs dont have adequate solutions to fix spoofing problems

Reactive Approach

Existing countermeasures are mainly based on reactive approach which cannot address the problem

Impact on Customers

Banks face customer Dissatisfaction, Penalties from regulators, etc.

Potential Social Engineering Fraud Scenarios

Calls with Spoofed CLI to Bank Customer

- Client receives fraudulent call that looks like regular call from known bank number
- Client trusts the caller based on known number and shares sensitive information

Calls with spoofed CLI to Bank Call Center

- Bank call center operator receives fraudulent call that looks like regular call from bank client
- Client is automatically identified based on valid MSISDN, and simplified authentication procedure is used

Scam Calls to Bank Client

- Bank client receives vishing call from fraudster
- Fraudster succeeds to convince client that call is legitimate and obtains sensitive information

Call to Bank Client Redirected to Fraudster

- Using vishing, fraudster already gained access to subscriber profile and has setup call redirect to own number

heksagon

PROTECT
INTERCONNECT
MONETIZE

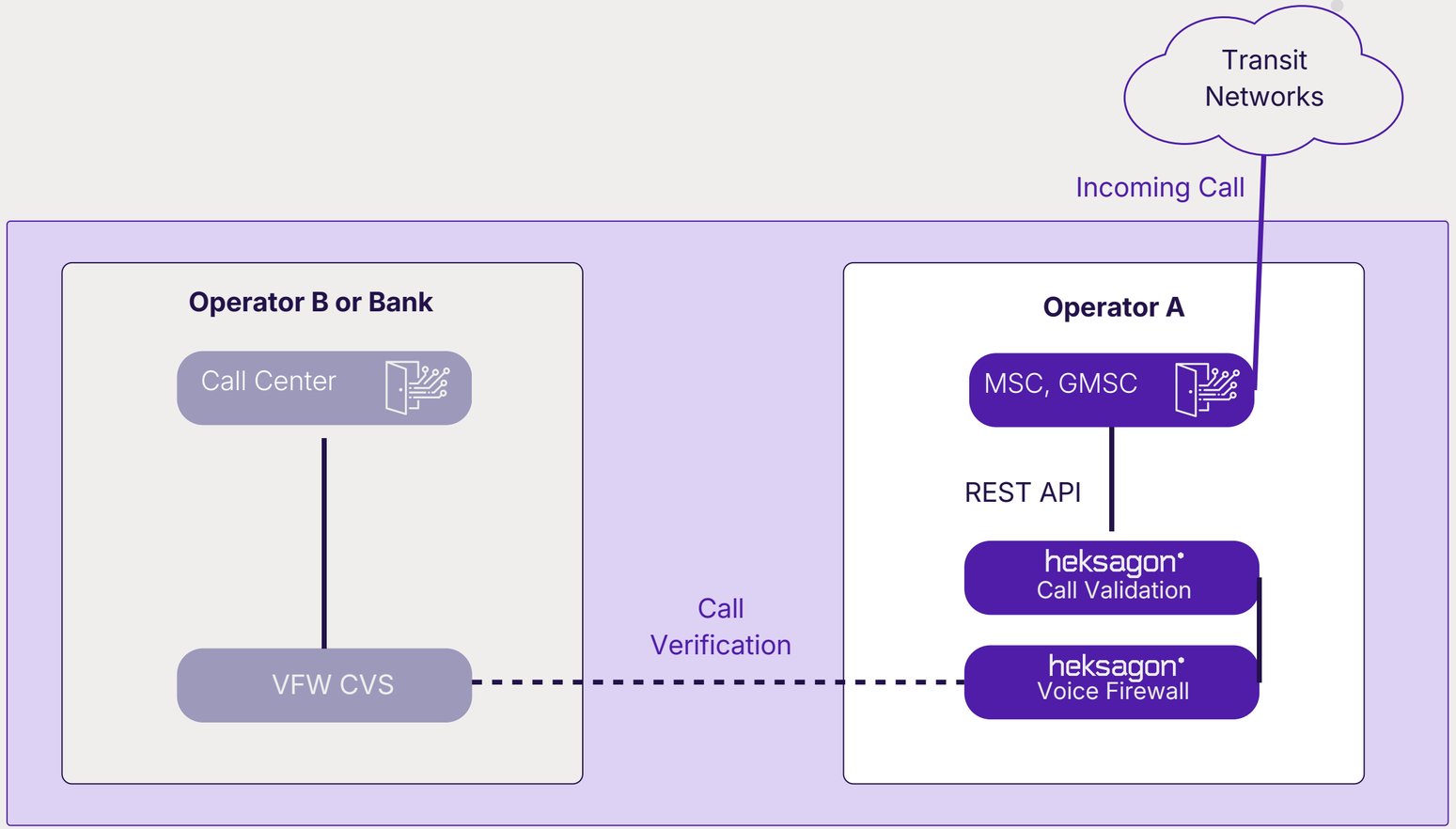
Heksagon Call Validation Solution

How Does Heksagon Call Validation Work?

- Real time verification of CLI with peer operators/banks and trusted enterprises (e.g., banks) to prevent spoofing and fraud.
- Blocks suspicious or fake calls - protecting subscribers from scams
- Enhances user trust, supports regulatory compliance, and creates monetization opportunities for operators

We are an Open-Source Call Validation Solution

(Capable of Inter-working with any 3rd party VFW)



E2E Fraud Protection

- CLI Spoofing
- Interconnect Bypass
- Impersonation fraud
- Social Engineering frauds

Advanced Spoofing Checks

- Dynamic Call Back
- Roaming On Call check
- Inter-operator call check
- Central DB

Revenue Protection & Generation

- Prevent revenue leakages
- Generate new revenue streams
- Commercial Service for MNOs

heksagon

Call Validation Solution

Basic Anti-Spoofing Checks

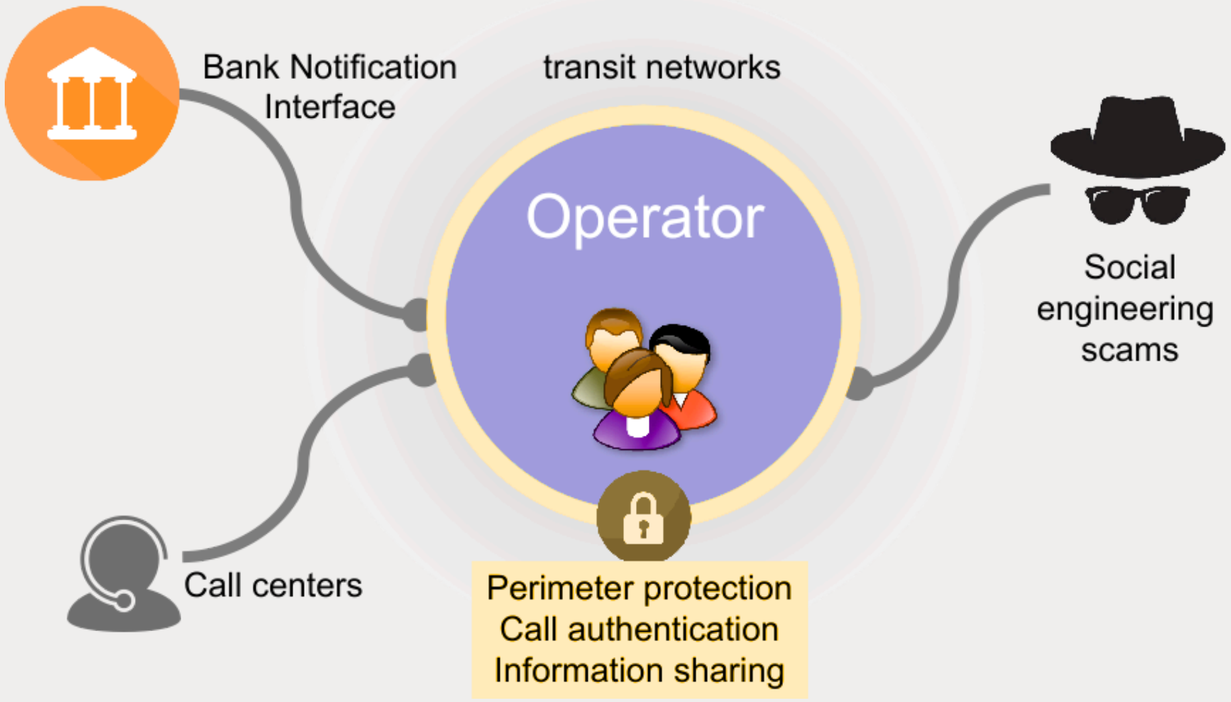
- Unallocated numbers
- Invalid CLI
- Control of impossible calls
- Roaming Check

Protection Beyond Telcos

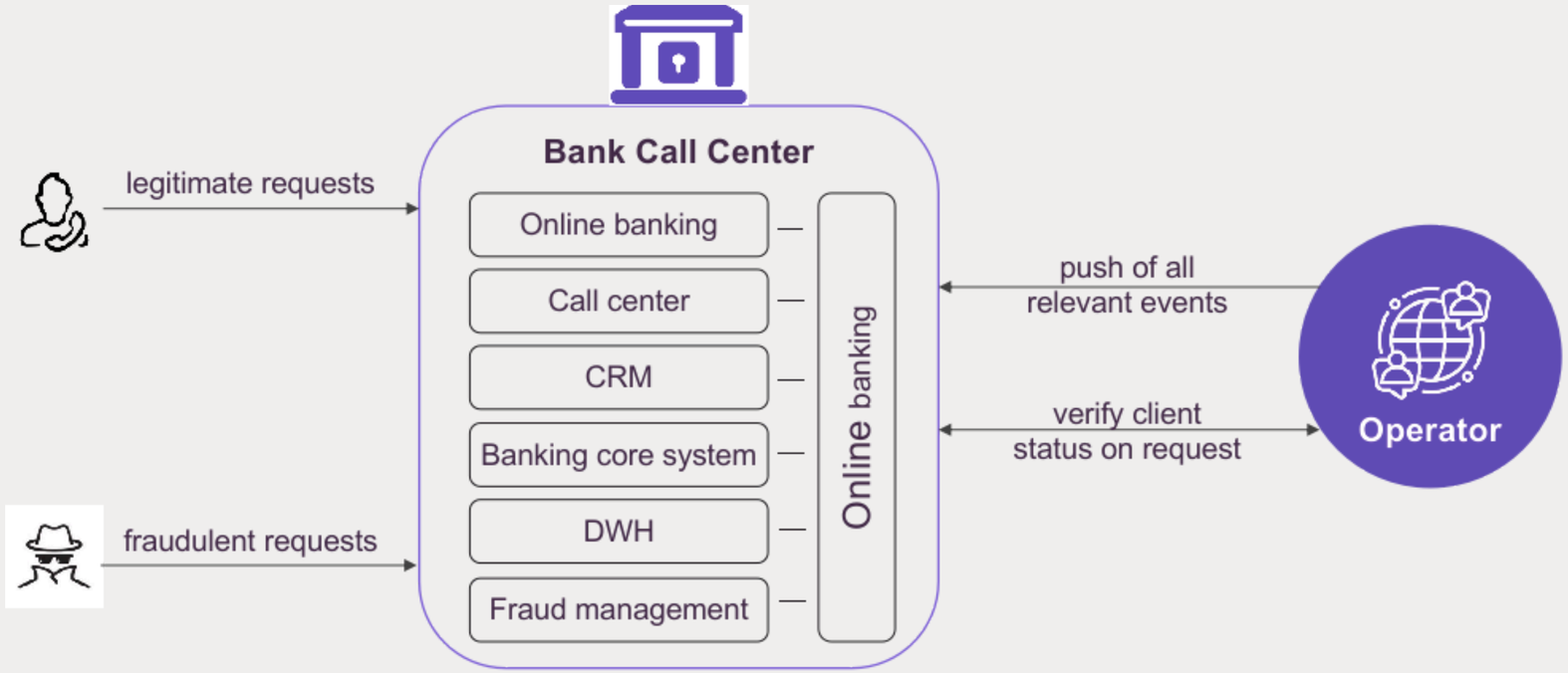
- “Bank” to client calls
- “Client” to bank calls
- Commercial Call Centers
- Government identity protection

How can Telecom Operators Help Banks Fight Voice Call Scams?

- **Identify high-risk operations which need to be protected**
  - Change of access data
  - Change of contact information
  - Transfer of funds
- **Establish interface with operators – one of following possibilities**
  - Validation interface (on request validation of subscriber state)
  - Collect proactively all events indicating potentially increased risk („push“)
- **Modify internal procedures to mitigate situations with increased risk**



Protection of Banks Against Social Engineering Fraud: Data Push



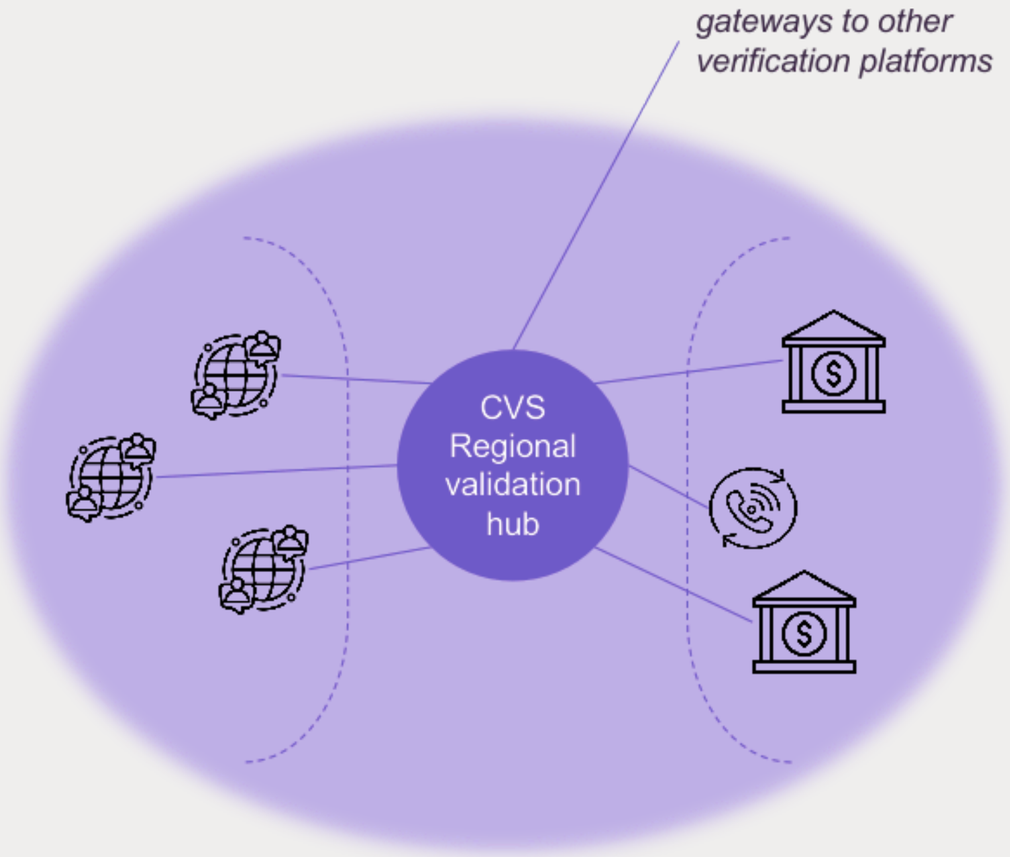
Prevention of Bank Social Engineering Frauds

Bank notification

- Real-time notification to bank about high-risk calls involving bank clients by data push or call verification

Perimeter protection (operator's network established as safe zone)

- Use of perimeter protection to statically detect and prevent calls that do not follow known routing of bank calls
- Use of perimeter protection with inclusion of bank call center in dynamic real-time call verification scheme to allow only authenticated calls



Prevention of Bank Vishing Fraud - 360 Protection

Real-Time Data Push to Bank

- Inform bank about call from known fraud number, spoofed CLI or redirected number to bank
- Inform bank about high-risk call involving bank client

Feedback to Bank Query About Current Client Status

- In case if any of high risk events happened in near past or is still in progress
- Client is involved in long conversation

Assure Validation with Bank Call Center

- Prevent calls from call center CLI not confirmed by bank
- Prevent calls from spoofed bank client CLI to bank call center

Deployment Requirements

MNO 

Pre-requisites:
- VFW deployed at MNO

Additional Scope:
- CVS Implementation
- Integration with Bank over API

Bank 

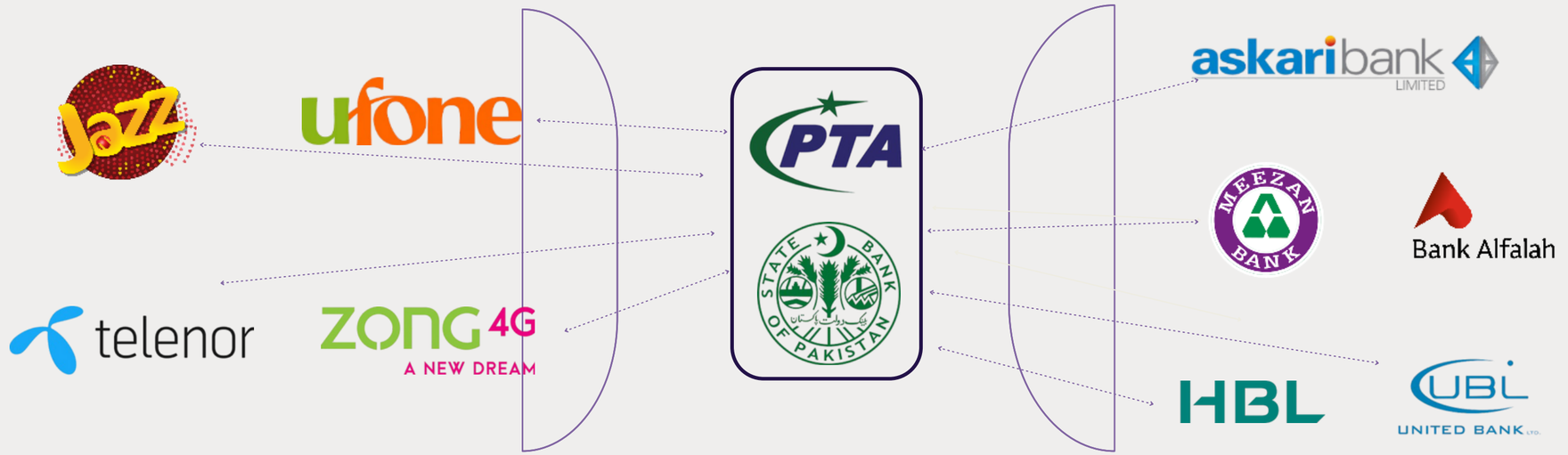
- Does the bank have any infrastructure installed at their premises? If no, then a light-weight VFW can be installed at bank premises.
- Integration of MNO VFW with Bank call center
- CVS Implementation with MNO over API

Note: For the sake of simplicity, it is possible to consider migration of bank traffic (backend number/bank UAN) to direct B2B voice interconnect connected with bank (PRI or SIP trunk group)

National Call Validation Hub Concept

Telecom Operators

Banks, Commercial Enterprises



Heksagon Voice FW solution (FCM) is already live with Ufone, Pakistan which supports call validation functionality

Call Validation service extended to banks and commercial enterprises etc.

Call Validation Benefits

Enhanced Network Security
Ensuring a fully protected environment

Revenue Protection
Preventing revenue losses and fraudulent activities

Improved Service Quality
Reducing number of subscriber complaints and improvide customer satisfication

Seamless Integration
Minimising operational disruption and ensuring immediate protection

Process Automation
Enabling effective call validation management without need for human intervention

Real-time Evaluation
Immediate reaction on any detected spooding case. Minimising the risk of false positives

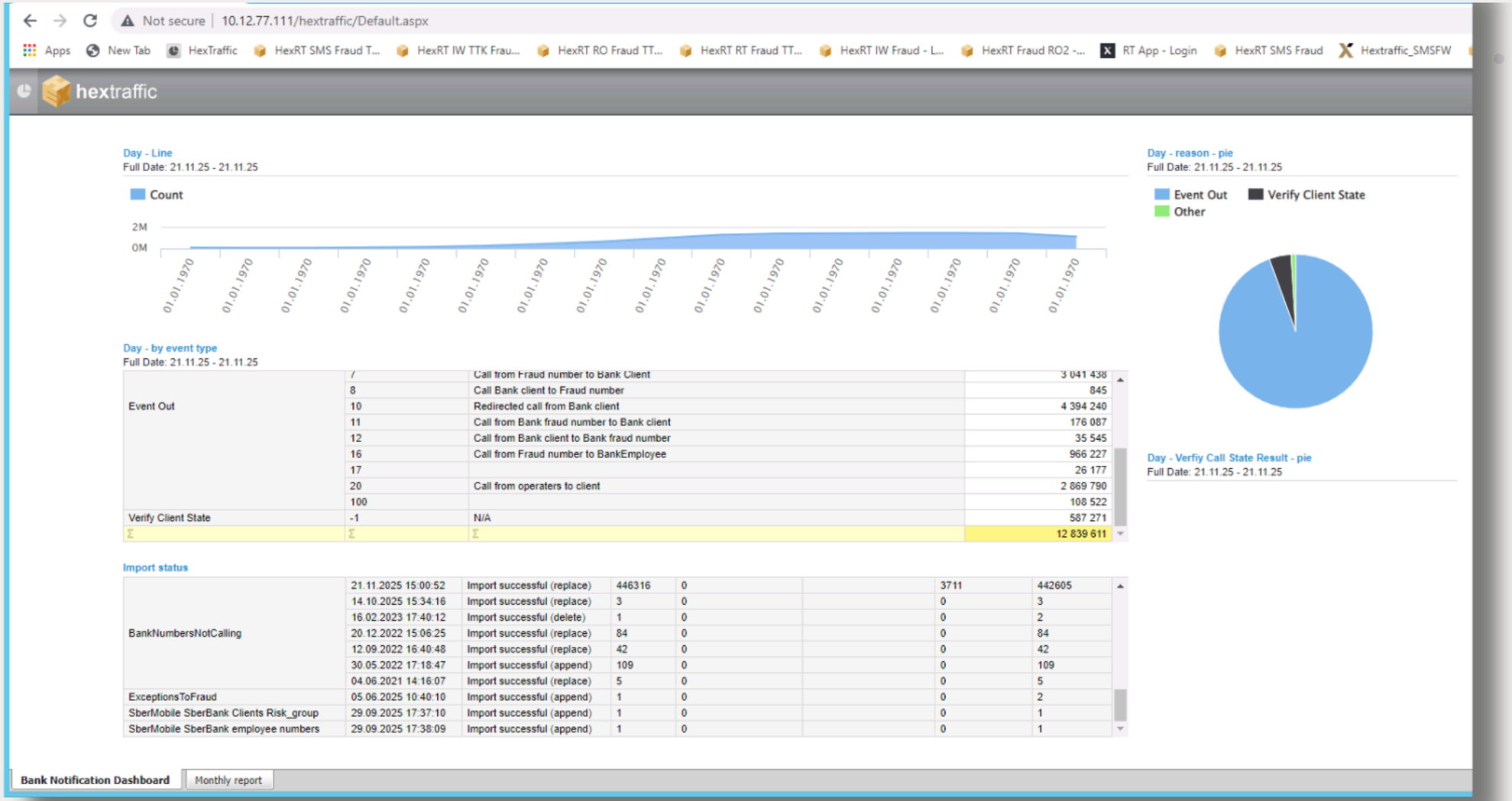
Reporting & Analytics

Following KPIs will be available for MNO and Bank management in the form of dashboard reports. Also, it is possible to further drill down to detailed data for further analysis for expert users

Suggested KPIs:-

- Number of calls from bank call center to bank clients verified by CVS (day, month)
- Number of calls from spoofed bank CLI blocked by MNO VFW (day, month)
- Number of real-time events reported to the bank by MNO VFW (day, month)
- Count of unique bank clients protected by the CVS solution in certain period (day, 1 month)
- Number of calls from subscribers to bank call center verified by CVS (day, month)
- Number of calls from spoofed subscriber CLI to bank call center not confirmed by CVS (day, month)

Reporting Module Snapshot



Example Call Validation Business Case

Revenue-Generating Service: Introduce a caller identity validation service offering for local bank to enhance security and trust

Item	Value
Number of Bank clients	40,000 (estimated)
Minimal monthly “Call Protection service” per client (Service Subscription fee)	$ 1.00
Monthly Revenue Earned	$ 40,000

Note: Heksagon is open to a minimal fixed fee per enterprise connection or a flexible revenue-share arrangement

Evolution Beyond Call Validation

360° Risk Profile Evaluation

Extension of AI risk model with other relevant data (calls, SMS, data service, SIM swap, device swap)

Deployment of Anti-Scam Module on Both Sides

Real-time scam prevention module in banks for enriching the risk profile with client banking data.

Silent Authentication

Use operator core network infrastructure to confirm identity parameters.

Compliance with Open API Concept

Wider reach and fast implementation by alignment with GSMA and CAMARA open NW API standards.

heksagon

PROTECT
INTERCONNECT
MONETIZE

Case Studies & Testimonials

Fraud Types Prevented

- **CLI Spoofing**
- **Interconnect Bypass**
- **SIMBOX**
- **Vishing**
- **Social Engineering**
- **Robo Calls & Spam Calls**

Tested and Approved

- Solution launch: 2019
- Pilot project and first customer onboarding: June 2019
- Actively protecting **65 million bank clients**
- Live with **9 different commercial banks**
- Deployment stage with **5 Mobile Operators in 3 countries**

Markets:

- Russia - Slovenia - Kazakhatsan
- Croatia - Tajikistan

Trusted by:

Kcell TelekomSlovenije TELE2 A1 telemach

...and over 30+ other MNOs worldwide!

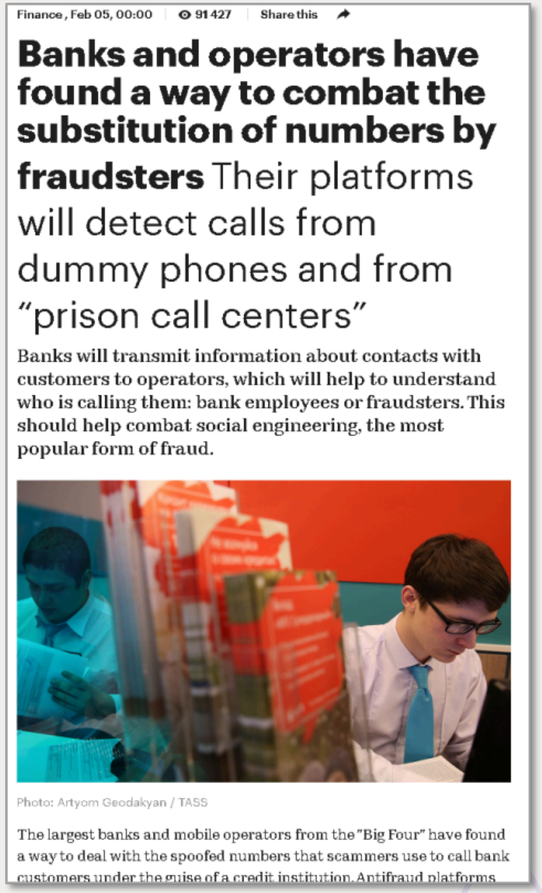
Benefits for Banks

- **Prevent Revenue Losses**
- **Improved User Experience**
- **Regulatory Compliance**

Experience with Implementation in the Russian Federation

- Operators offered an active support to the banks to fight this type of fraud – Megafon, MTS and Tele2 are using hexCVS to provide this service to banks (Tinkoff, Sberbank and several other in evaluation stage)

- Interface to banks is using standardized API to hexCVS call verification solutions



Finance , Feb 05, 00:00 | 91 427 | Share this

Banks and operators have found a way to combat the substitution of numbers by fraudsters Their platforms will detect calls from dummy phones and from "prison call centers"

Banks will transmit information about contacts with customers to operators, which will help to understand who is calling them: bank employees or fraudsters. This should help combat social engineering, the most popular form of fraud.

Photo: Artyom Geodakyan / TASS

The largest banks and mobile operators from the "Big Four" have found a way to deal with the spoofed numbers that scammers use to call bank customers under the guise of a credit institution. Antifraud platforms

Testimonial

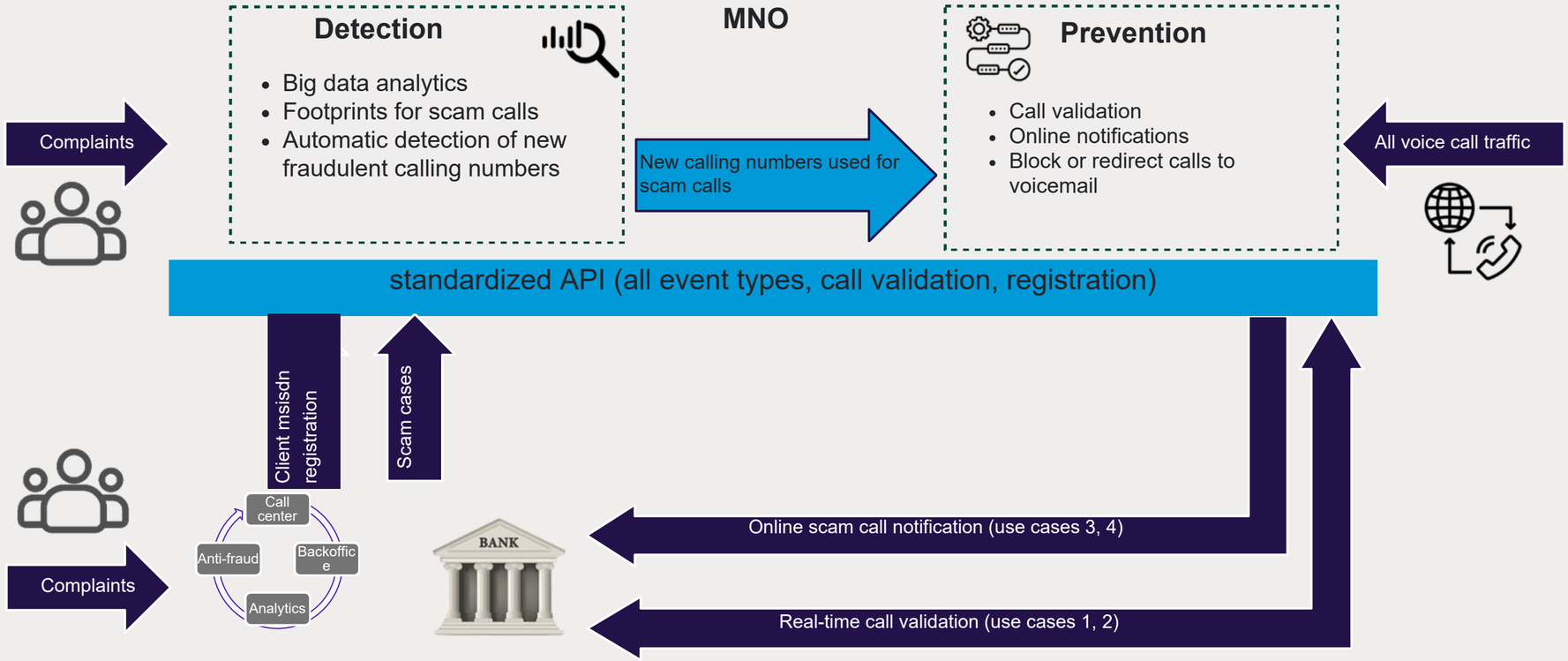
CVS solution enabled detection and prevention of 80% of incoming fraudulent calls...

Tinkoff Bank

In year 2020 we recorded 3,4 million complaints yearly related to CLI spoofing. This number was significantly reduced with introduction of CVS platform and overall combined with internal fraud prevention procedure the financial impact of those attacks was reduced by 2,5 million USD quarterly.

SberBank

Call Validation: Social Engineering Prevention - Solution Online



heksagon

PROTECT
INTERCONNECT
MONETIZE

Powering the Future of Telco Operations:

- Fraud Detection and Prevention
- Routing and Interconnect Management
- Flash Call Prevention and Monetization

About Heksagon:

Heksagon is one of the leading software development firms specializing in telecommunications, with a foundation dating back to 2007. Together with its affiliated companies, Heksagon has established a robust presence in the IT and telecommunications industries. Our solutions are implemented by telecom operators in more than 20 countries, serving both small and large-scale operators.

Get in Touch:

www.heksagon.com
info@heksagon.com

Follow Us!

Global Offices and Contact:

- Belgrade, Serbia: +381 69 10 80 922
- Munich, Germany: +49 32 223270037
- Islamabad, Pakistan: +92 344 5771970
- Astana, Kazakhstan: +7 705 688 93 66