XFraud
Telephony Abuse

Telephony abuse prevention and suppression

XFraud is an XCarrier platform application module that detects fraudulent activities from the public telephone network and proactively prevents or suppresses them according to certain rules.

Carrier switch infrastructures are automatically monitored in real time by the XFraud application and provisioned accordingly as required. XFraud efficiently and proactively protects carriers and end customers from fraudulent telephone activities. The protection opens up trunks or A-number and B-number bases.

At the same time, push notifications via email, SMS or proactive trouble tickets alert teams that are responsible for operation.

Terms and Definitions

Telephone and Communication Fraud
Telephony fraud or communication fraud is where telecom services and products are used with the intention of illegally obtaining money from carriers or their end customers or avoiding paying them. Sophisticated technology is often used to exploit victims' faulty infrastructures.

What kind of fraudulent activities does XFraud combat? (Key examples, not exhaustive)

- Abuse fraud based on origin and/or destination telephone numbers
- Hacking of PBX/local telephone exchanges and misuse of telephone numbers
- Wangiri callback (ring once) from foreign premium rate numbers to obtain a dialing tone
- Arbitrage/tromboning – calls routed back to the country of origin via the foreign country
- International revenue share fraud (IRSF) – abuse of premium rate numbers.

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

Identifying Fraud

- Telephone traffic arriving on an operator's carrier switches and interconnection trunks is continuously checked for specific telephone numbers, format, plausibility, volume, origin, destination, time and other specific parameters.
- As part of this, various references are used as a basis for specific protective actions.
  - **Lists**: known fraudulent origin or destination numbers or ranges of numbers are automatically blocked.
  - **Call volume and pattern**: unknown, sudden sharp increases in telephone volumes are detected immediately.
  - **Call times**: sharp increase in call volumes at unusual times of the day or on unusual days are suspicious and are analyzed accordingly by XFraud, learned and, if necessary, alerted or even prevented.
- XFraud also uses internal operator sources to detect fraudulent calls. Incoming call data records (CDRs), for example, are analyzed by carrier switches in near real time and processed by an extremely wide variety of rules, logics and algorithms instantly.
- Newly discovered rule violations or unusual patterns are identified and appropriate rule actions are immediately applied to specific telephone number(s) or trunks.
- Country-specific, additional, external sources of information are dynamically available depending on the area of application (country) and regulation. When available, they are connected electronically via API and integrated into the processing logics.
- Additional, manual entries can be made using the graphical user interface at any time, either as an additive or a complementary solution.

Operation and Interfaces

- XFraud is configured and operated using XCarrier's graphical user interface (GUI).
- The following common import file formats and data collection protocols are currently in use. The following list is not exhaustive.

Import Formats	**Data Collection Protocols**
• .xls	ftp, sftp
• .csv	http, https
• Json	SOAP
• Xml	REST
• Dblink	…
• …	

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

Automated Protection Actions

XFraud acts based on preconfigured action plans and self-learning algorithms

- Defined, dynamic lists with registered numbers or ranges of numbers
- Alerts via SMS, email and push notifications
- Automatic opening of trouble tickets
- Automatic switch provisioning and list enrichment of numbers/trunks to be blocked
  - Blocked numbers and trunks are marked uniquely and with a time stamp so that they can be post-processed

The XFraud Traffic Profiler is a logical control unit

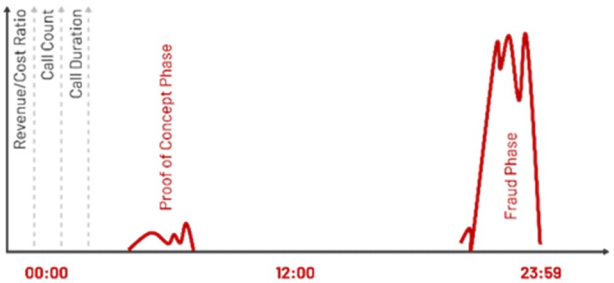
- Threshold and alerting values are defined per month, day and hour, for example. Continuous comparisons with reference or historical data are conducted.
- Ad-hoc tests can also be performed manually in live mode. If required, individual rules can also be activated/deactivated in live mode.
- Destination screening using volume thresholds are also available as high-usage monitoring.

Reports by Phone Number, Customer and Destination

- XFraud produces statistical tables or graphical reports that assist users in manually identifying and narrowing down any qualifications of fraud.
- Fraudulent activities often start with a test at a usual time of day (proof of concept phase). The actual fraud then intentionally takes place at times when operational teams at carriers and service providers most likely won't be working.
- Fraudsters commercially exploit surprise effects. XFraud helps operational teams with automatically detecting patterns and automatically initiating any necessary switch blocking. Appropriate push notifications are sent.

Reporte	15.02.2021	19.11.2021	03.12.2021
Destination	**Chad-Mobile**	**Ukraine-Mobile**	**Estland-Mobile**
Call Duration	**1526.05**	**20.30**	**2533.02**
Amount Rate	**998.94**	**20.65**	**1612.30**
Cost	**0.00**	**0.00**	**0.00**
Start Count	**1675**	**7**	**2628**
Unanswered Count	**38**	**2**	**57**

- Fraudulent activities often start with a test at a usual time of day (proof of concept phase) and in small, inconspicuous quantities.
- The actual fraud then intentionally takes place at times when operational teams at carriers and service providers most likely won't be working, e.g. at night or on weekends and public holidays.



Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

Customer Added Value

Added Value for Carriers

- Compliance with regulations (e.g. laundering illegal money).
- Boost to carrier brand identity due to communicated and effective customer protection.
- Prevention of financial claims and damages.
- Secured sales and margins.
- Lower cost of ownership.

Added Value for Carriers end Customers

- Protection of private and business end customers from voice fraud.
- Preventive and additive security shield for end customers.
- Prevention of financial damage.

By using Carrier Call AG's XFraud system, we can proactively protect our customers from large financial losses. We're the only company in Switzerland to offer this service.

Josef Furger
Senior Product Manager B2B, Sunrise UPC

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com