Stop worrying about SIM Swap fraud with Cleafy

Fraud management solution for banks and financial institutions

Banking | Financial Services | Crypto Exchanges

A **SIM Swap fraud** is when the fraudster gains access to the victim's mobile number to receive OTP messages, bypass MFA, and finalise an **Account Takeover** (ATO).

Criminals **steal the victim's number** by impersonating the victim and asking the mobile network provider either a SIM card replacement or a mobile number trasfer. This scam usually works because of **poor controls** put in place by the mobile network providers staff, or **lack of strict regulations** around SIM replacement processes. As they previously gathered the victim's personal data (such as phone number and online banking credentials) via **social engeeniring tecniques**, once they stole the victim's mobile number, criminals have everything they need to attempt an ATO.

As in the case of **phishing attack**, SIM Swap cannot be prevented itself but the Account Takeover attack that follows can.

Cleafy is a new generation **all-in-one platform**, which features all the key capabilities needed to detect any type of ATO **attempt**.

SIM Swap fraud

How does Cleafy detect an ATO attempt following a Sim Swap?

By observing the following anomalies and correlating them, all in real-time.

Behavioral Analysis Anomalies

- New device
- New network
- Abnormal biometric behavior
- New location

Transactional Analysis Anomalies

- New payee
- Transaction outside the user's spending profile
- Abnormal number of transactions
- New country to which the transfer is being made

Device Intelligence Anomalies

Number of users from that device: too many users logging in from the same device is a very high risk indicator.

Moreover, **Cleafy correlates everything** with the fact that an SMS was requested as a means to receive OTP.

And this is the **strength of Cleafy**: correlating a myriad of indicators to detect fraud attempts, without creating unnecessary friction for the end user.

Cleafy has proved extremely efficient in automatically detecting and stopping ATOs.
The strengths that allow Cleafy technology to achieve this efficiency are:

User prediction capabilities	Cleafy's **ML algorithms** exploit a myriad of behavioral and biometric information to predict the actual user identity with high accuracy, even before the authentication is completed.
Malware detection capabilities	Cleafy **patented full content integrity** detects the slightest tampering within the content of the app or web-app, even in the case of **0-day malware**.
Risk propagation	A **patented feature** that allows Cleafy to automatically propagate the risk detected on the victim's device to that of the fraudster to intercept ATO scenarios through malware.
Tailored Threat Intelligence	Cleafy engine is constantly enriched with the information gathered by the Cleafy **Threat Intelligence Team**. The patform allows access to the details of the most advanced ATO schemes, and automatically detect and label them.
Adapative response via smart rules	Once identified the various patterns and evidence of anomalies, Cleafy allows you to **set up targeted responses** to the customer's needs.

Benefits for you

Complete control of risk

Lower fraud impact

Lower friction for users

You look ahead, we've got your back

+25
Patented Technologies

+60 Million
Daily Protected Online Users

$700 Billion
Protected yearly

Gartner peerinsights™

Cleafy's rating
4.9 ★★★★★
based on all published reviews

Head of Security
Top 3 European bank

"Cleafy represents our single-point fraud management solution, providing us with everything we need to detect sophisticated attacks to our online services."

CISO
Top 10 European bank

"Thanks to Cleafy we can detect targeted attacks, prevent frauds, and reduce false positives; the efficiency of our small anti-fraud team has largely improved."

To learn more about how we can **help you stop worrying about SIM Swap by protecting you from Account Takeover** contact us or download our Cleafy Solution Overview.