telesign

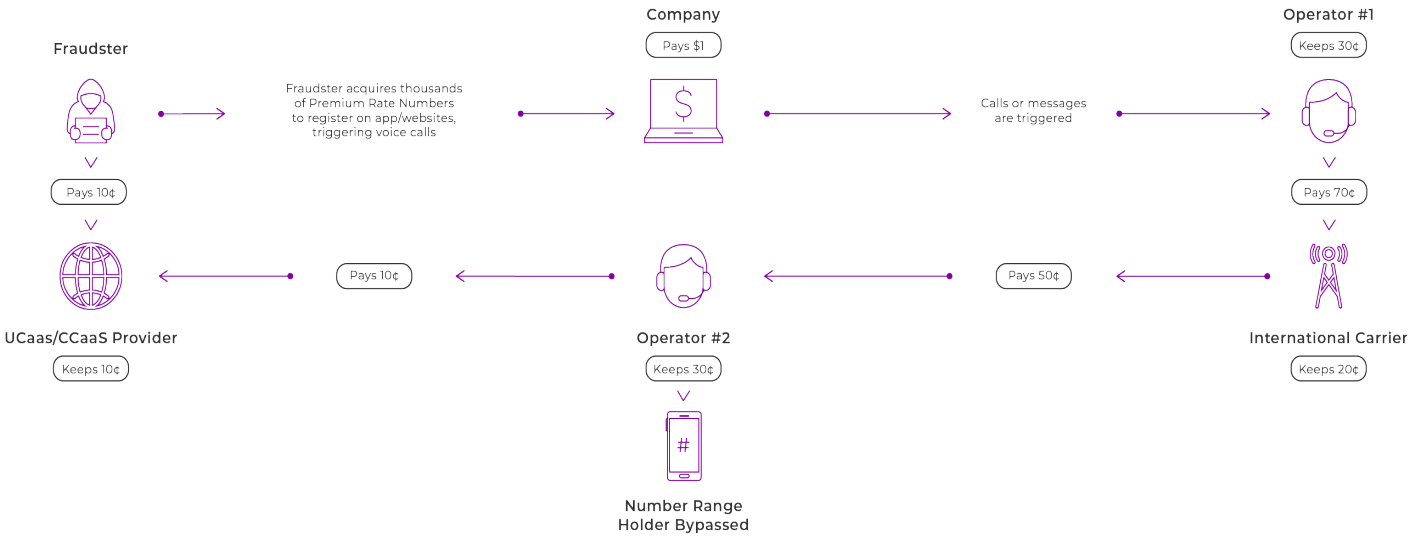
SOLUTION BRIEF

IRSF: International Revenue Share Fraud

Identify IRSF in its tracks

IRSF attacks target companies that generate a high volume of calls and text messages to their customers, such as call centers or online businesses that use SMS one-time passwords (OTP) as part of their sign-up process. An indication of IRSF is when a spike in volume of text attempts to phone numbers in different regions of the world occurs. Another vertical to consider is the velocity of text attempts that are coming in. If you see one text attempt every second, with velocity of the text attempts changing to fifty text attempts in one second, this indicates fraudulent activity.

How IRSF works



1. Fraudster illegally acquires thousands of Premium Rate Numbers or number ranges to register on app/websites, triggering voice calls and/or messages

2. Fraudster initiates automated scripts to cycle between the numbers in their range. They might test the scripts with a few transactions to see if it gets terminated and then build up or burst traffic to those ranges

3. Fraudster colludes with IPRN providers and content providers to carry out artificial inflation of traffic from acquired numbers

4. Fraudster will continue to move on to another number or another destination to carry on the traffic until the number ranges are blocked by the originating home operator

Who's at risk?

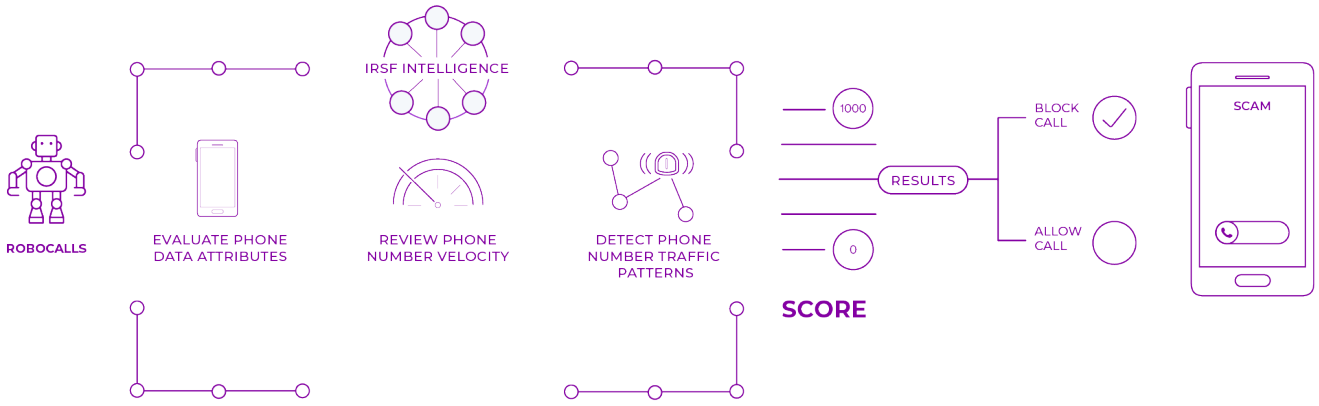
UCaaS & CCaaS providers

UCaaS and CCaaS providers face challenging risks which are impacted with fraud through several methods including inbound & outbound call fraud, PBX hacking, and callback fraud.

Online businesses

Since the pandemic began, online registration process flows quickly grew, overwhelming with consumer traffic. Fraudsters quickly identified this vulnerability and began targeting digital online businesses with account registrations involving rich notifications, OTP requests, and more.

Defect & defend against MFA & communications frauds



Dedicated machine learning model

Draw on 15+ years of historical data patterns and supporting analytics. Our dedicated IRSF machine learning algorithm delivers continuous performance improvement that grows and adapts to your business.

Real-time decision making

Harness billions of identity signals, traffic patterns, and a global fraud consortium and receive a dynamic risk-based assessment score. Allow or Block SMS OTPs and voice calls within a matter of milliseconds.

Immediate results

Save time and money.
Plug our developer-friendly API into your fraud prevention stack or verification framework.
The model is already trained and ready to make an immediate impact.

Sources:
1. Proximus Group

telesign