telesign | bics | routemobile

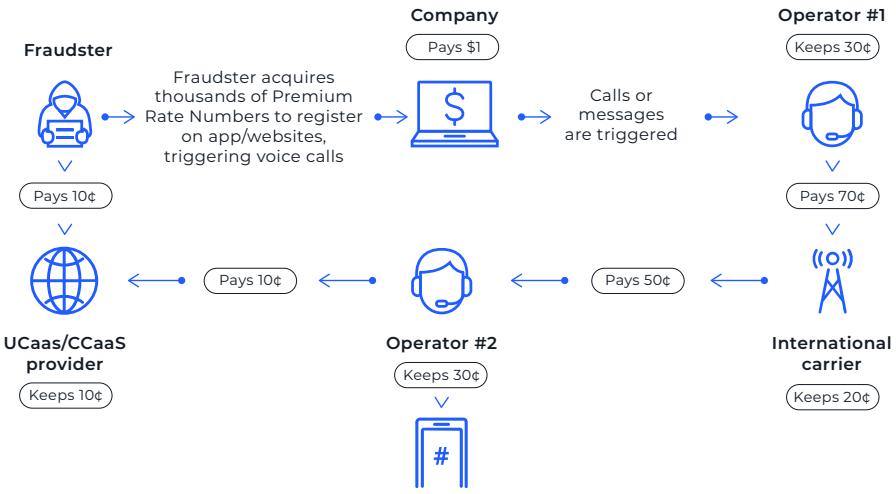
Proximus Global

Solution Brief

IRSF Intelligence: The most expensive fraud you've never heard of

IRSF has quickly become the most menacing type of communication fraud for businesses today. Fraudsters unethically obtain a range of premium rate numbers and target companies that generate a high volume of calls and messages via call centers, SMS or voice one time passwords, and more. Sophisticated attacks inflate traffic across the number ranges and siphon money from every interaction. IRSF attacks happens in a matter of minutes and cost businesses $50k per attack, on average.

How an IRSF attack operates



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.

Recognize critical IRSF behaviors before they recognize you

- Abnormal behavior across number ranges
- Unusual volume of calls or messages coming to or from risky countries
- Unusual volume of calls or messages coming to or from premium rate numbers
- Bot and machine-like activity
- Number belongs to a high-risk carrier
- Number is a premium rate number

Who's at risk?

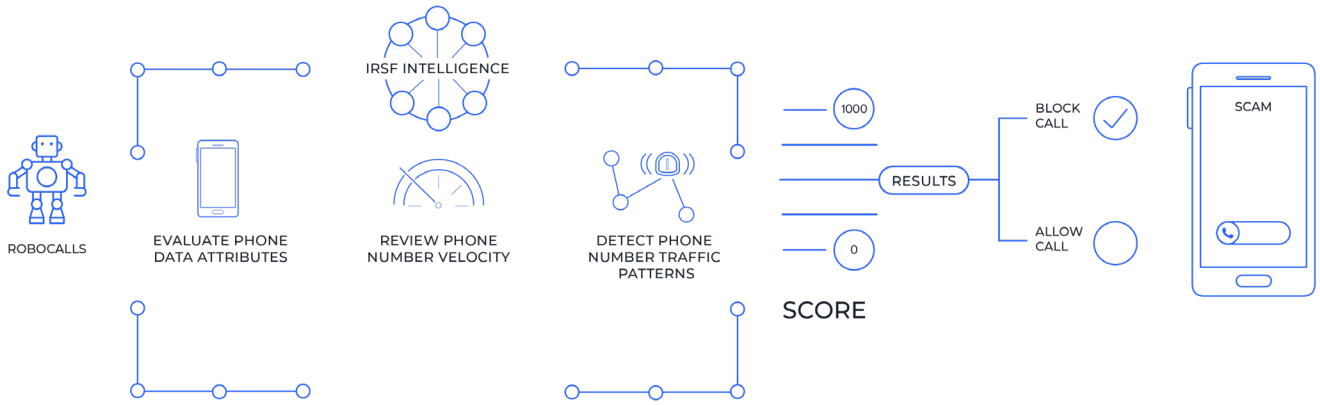
UCaaS & CCaaS providers

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

Online businesses

Since 2020, online registration processes quickly grew and became overwhelmed with consumer traffic. Fraudsters quickly identified this vulnerability and began to target online businesses with account registrations involving rich notifications, OTP requests, and more.

Deflect & 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. Leverage an insightful dashboard with visual reporting, subscription management and system alerts

Proximus Global, combining the strengths of Telesign, BICS, and Route Mobile, is transforming the future of communications and digital identity. Together, our solutions fuel innovation across the world's largest companies and emerging brands. Our unrivaled global reach empowers businesses to create engaging experiences with built-in fraud protection across the entire customer lifecycle. Our comprehensive suite of solutions – from our super network for voice, messaging, and data, to 5G and IoT; and from verification and intelligence to CPaaS for personalized omnichannel engagement – enables businesses and communities to thrive. Reaching over 5 billion subscribers, securing more than 180 billion transactions annually, and connecting 1,000+ destinations, we honor our commitment to connect, protect and engage everyone, everywhere.

Learn more at **proximus.com/proximus-global**