infobip

BSP Circular 1213:

Building a fraud prevention framework Philippine banks can stand behind

43% of Filipinos have been targeted by digital fraud. For banks, that's a customer retention problem before it's a compliance one.

75% of banking customers say they'd switch institutions if fraud were managed badly. BSP Circular 1213 has added regulatory pressure to what was already a market and reputational imperative.

What BSP Circular 1213 requires

Issued in June 2025 under AFASA, Circular 1213 applies to all BSFIs with aggregate monthly transaction values of ₱75 million or above. It defines 5 capability areas.

- **Fraud management systems.** Real-time monitoring and detection infrastructure that can identify and block suspicious transactions as they occur.
- **Strong authentication.** A move away from SMS and email OTPs toward biometric, behavioral, and adaptive authentication that adjusts based on transaction risk.
- **Account safeguards.** A mandatory 24-hour pause after key account changes, and a prohibition on sending clickable links or QR codes through SMS or messaging apps.
- **Real-time notifications.** Transaction alerts sent immediately through secure channels with enough detail for customers to verify or dispute activity on the spot.
- **Fraud detection and response.** Automated systems that go beyond detection to enable immediate threat response.

Detection alone isn't enough. This guide covers the communication, verification, and response layer that sits on top of existing fraud infrastructure and makes it work for the customer.

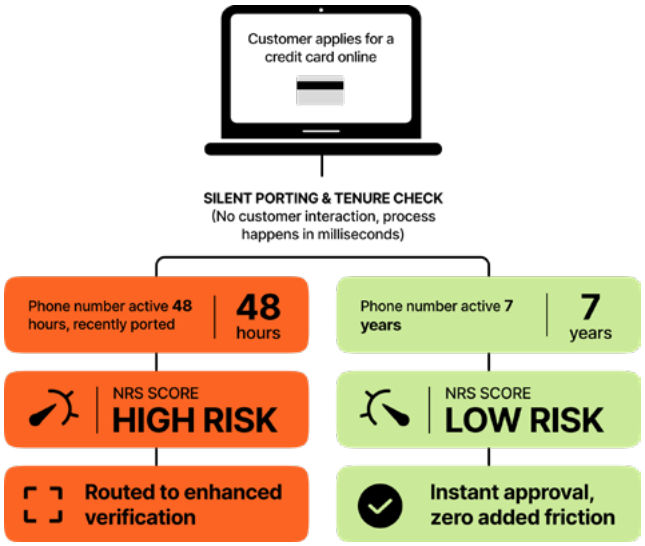
Four moves to strengthen your framework

1 PROTECT

What a phone number can tell you before you trust it

Number risk scoring

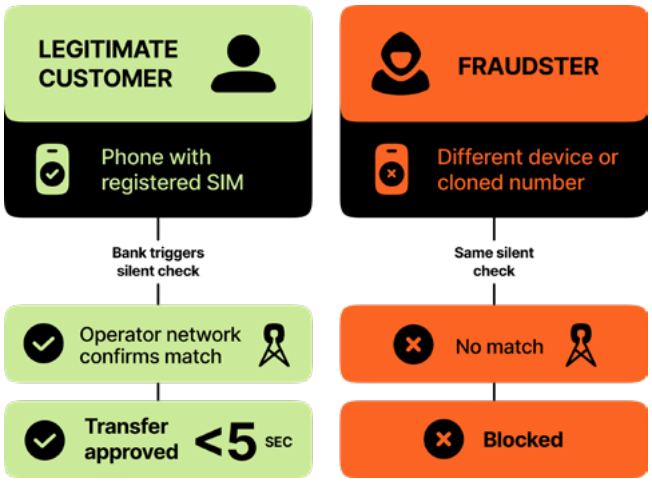
When a phone number first enters the system, Number Risk Scoring (NRS) answers whether you can trust it. It evaluates real-time and historical signals, how long the number has been active, whether it was recently ported, unusual activity patterns, and returns a risk score banks can act on immediately. Legitimate customers move forward with no extra steps. High-risk numbers are flagged before damage is done.



Silent network verification

Network APIs verify identity at the operator level, with nothing required from the customer. Number Verify confirms the registered SIM is in the device making the request, in under 5 seconds. No code sent, no OTP, nothing to intercept. SIM Swap Detection flags whether a number's SIM has been recently changed, adding a critical signal before any high-value transaction proceeds.

The same ₱200,000 transfer. Two very different outcomes.



Secure OTP delivery and push authentication

Where OTP is still needed, Viber OTP delivers it through an encrypted channel with the bank's verified profile visible, making phishing attempts immediately distinguishable. For banks ready to go further, push-based authentication replaces OTP entirely: customers approve transactions directly in the banking app using biometrics or PIN, with no code generated and nothing to intercept.

2 NOTIFY

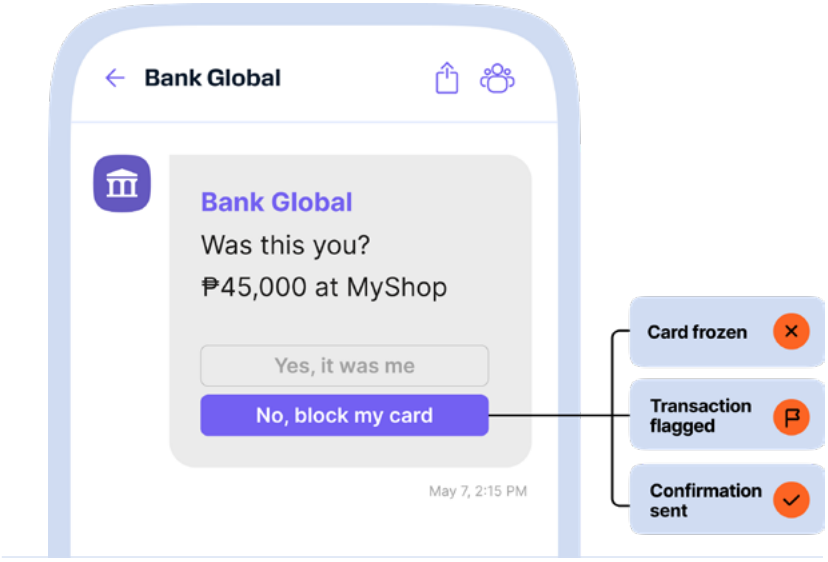
Get the right alert to the right customer in seconds

Alerts route to the customer's preferred channel with automatic failover. If Viber fails, the alert moves to SMS. If SMS fails, it moves to push. Every alert carries full transaction context so customers can confirm or flag activity immediately. Verified business profiles on Viber, WhatsApp, and RCS ensure every message arrives with the bank's authenticated identity, making the bank's communications instantly distinguishable from phishing attempts.

3 AUTOMATE

Resolve cases and educate customers at scale

When suspicious activity is detected, customers receive an interactive alert asking them to confirm or deny the transaction. If they deny it, the card is frozen and the transaction blocked automatically, in seconds, without agent involvement. Viber and WhatsApp support interactive buttons natively, so customers respond directly in the message thread with no redirects and no links, fully compliant with Circular 1213.



Under 30 seconds. No branch. No queue.

4 ESCALATE

Step in when automation isn't enough

Complex cases route to a live agent via chat, Viber Business Calling, or WebRTC, with full conversation context handed over automatically. The escalation path should be designed, not improvised. Banks that build it deliberately turn a potential failure point into a differentiator.

Where to start

None of these capabilities replace what banks already have. They strengthen it. Number Risk Scoring, improved notification delivery, and operator-level verification for high-risk transactions are each viable entry points with immediate compliance and experience value.

With 800+ direct operator connections globally and support for 30+ channels, Infobip is built for the delivery reliability that fraud communication requires.

Talk to us about BSP Circular 1213 readiness.

Recognized by the experts

FAST COMPANY

Infobip named to Fast Company's Annual List of the World's Most Innovative Companies of 2024

Gartner

Gartner® Magic Quadrant™ for CPaaS 2025

Infobip is named a Leader

JUNIPER RESEARCH

Mobile Messaging Fraud Prevention Established Leader 2025

Conversational AI Established Leader 2025

RCS Business Messaging Established Leader 2026

OMDIA

Omdia Universe

CPaaS Leader 2025

IDC

IDC MarketScape

CPaaS Leader 2025

FROST & SULLIVAN

Frost Radar™: CPaaS

Infobip is named a Growth and Innovation Leader 2025

infobip

www.infobip.com