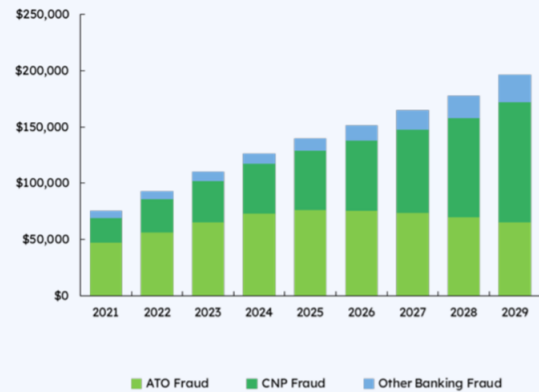


Prevent **SIM Swap** attacks using network signals

NOKIA

Mobile phone numbers are central to securing financial services, but this reliance makes them prime targets for fraud. **SIM swap fraud** occurs when a malicious actor convinces a mobile carrier to transfer a victim's phone number to a SIM card they control. Similarly, mobile number portability fraud reroutes a number without the owner's knowledge. Once successful, attackers intercept critical two-factor authentication (2FA) codes, gaining unauthorized access to bank accounts and digital platforms.

Total Losses to Fraud (\$m), 2021-2029



Source: Juniper Research report

The scale of this issue is alarming:



According to Cifas' **2025 Fraudscape report**, UK SIM swap incidents surged by **1,055% in 2024**, rising from 289 to nearly 3,000 cases, with estimated losses exceeding **£5.35 million**.



Juniper Research projects that the value of bank fraud in the U.S. will rise from **\$4.1 billion in 2029**.



Currently, less than **1 in 200** SIM swap attempts are flagged as fraudulent, highlighting a significant vulnerability.

Nokia's SIM Swap API: Real-time protection against Account Takeover (ATO)

Nokia's Digital Identity and Anti-Fraud solution, part of the **Network as Code** platform, provides a powerful API specifically designed to combat SIM swap attacks by leveraging real-time signals directly from the network.



How Nokia's SIM Swap API works

The SIM Swap API enables applications to instantly verify with the network if a recent SIM swap (change in SIM card associated with a phone number) has occurred. This check is integrated into critical user flows:

01

User login:

The user enters login credentials into the application.

02

Authentication check:

The application initiates authentication to verify user credentials.

03

SIM Swap check:

The application calls the SIM Swap API to check with the carrier if a SIM change occurred recently for that phone number.

04

Authentication successful:

If no recent SIM swap is detected, the user is successfully authenticated. If a SIM swap is detected, the application can trigger additional security measures or block the transaction.

Key benefits of Nokia's SIM Swap API:



Prevent SIM Swap attacks:

Instantly detect and prevent fraudulent activities stemming from SIM card changes.



Prevent Account Take-Over fraud:

Gain real-time visibility on user SIM status to protect against account takeover.



Real-time visibility on user SIM status

Access immediate information directly from the network regarding SIM card changes.



Prevent fraud losses

Protect against account takeover (ATO) fraud with real-time signals directly from the network, specifically preventing SIM swap-based attacks before they impact your customers.

“This approach is seamless. It’s a behind-the-scenes check that doesn’t add hassle for customers.”

Andy Stegner | AT&T

Why choose Nokia for SIM Swap prevention?

Simplified Integration

Use a single SDK to integrate network capabilities into your application that work globally, requiring no extensive network knowledge.

Technology You Can Rely On

The Network as Code platform boasts 99.999% historical uptime and has managed 80 billion API calls.

Trusted Network Data

Leverage direct, real-time insights from the network to enhance security and create secure, frictionless customer experiences.