Digital identity verification and fraud detection

Through the power of the network

Nokia Network as Code

NOKIA

Consumer fraud losses in USA in 2024[1]

$12.5B

Total fraud losses in European Union in 2023[2]

$4.6B

Account takeover fraud experienced by merchants[3]

32%

Identity theft fraud experienced by merchants[3]

36%

Digital identity: Securing the trust anchor of our hyperconnected future

In today's hyperconnected world, digital identity protection and fraud prevention have become fundamental pillars for maintaining trust in digital interactions and transactions. As societies become increasingly digitalized, with billions of connected devices and countless daily digital transactions, protecting digital identities has evolved from being merely a security concern to a critical foundation for social and economic functioning. According to the World Economic Forum's Digital Identity report, nearly 60% of global GDP is digitalized, making robust digital identity protection essential for sustainable digital growth.

Financial fraud, including mobile fraud, continues to rise and evolve at unprecedented levels globally, leading to significant losses for individuals and financial institutions. The Federal Trade Commission (FTC) recently released a report which highlights that consumers lost over $12.5 billion to fraud in 2024, marking the first time fraud losses reached that level.

Further, the exponential growth of Gen AI has lowered the entry barrier for criminals to exploit weaknesses in mobile payment systems, apps, and SMS-based authentication and launch highly personalized attacks such as identity theft, SIM swapping, and phishing.

According to Juniper Research, losses from online payment fraud could exceed $362 billion globally by 2028.

1: Federal Trade Commission (Consumer Sentinel Network Data Book 2024) | 2: European Banking Authority. 2024 report on payment fraud | 3: 2024 Global Payments and Fraud Report Merchant Risk council

The Identity puzzle: Traditional methods are falling short

In today's digital landscape, organizations face unprecedented challenges in verifying user identities and detecting fraud. Traditional methods like passwords, security questions, and basic KYC (Know Your Customer) procedures are increasingly inadequate. Fraudsters have become sophisticated, using synthetic identities, deepfakes, and stolen credentials to bypass conventional security measures. Moreover, static verification methods struggle to keep pace with the dynamic nature of digital fraud, leading to both false positives that frustrate legitimate users and missed fraud attempts that cost businesses billions annually.

Common limitations of traditional digital identity verification methods

Cost and complexity of traditional Know Your Customer (KYC) processes

Multi-factor authentication introduces friction

- SMS OTP not beneficial for user experience and can be deprecated

Lack of trusted real-time signals for fraud detection

- GPS and IP spoofing can falsify actual user location

No visibility on network device status changes

- Identifying SIM swap
- Identifying call forwarding to unknown number

Protecting digital identity through network intelligence

In today's hyperconnected world, digital identity has become a cornerstone of our daily lives. From online banking and shopping to accessing healthcare and government services, our digital identities enable us to interact seamlessly with various platforms and services. However, this reliance also brings significant risks, including identity theft, fraud, and privacy breaches. Protecting digital identity is paramount to ensuring secure and trustworthy interactions in the digital ecosystem.

Can the network help ?

Network intelligence offers a unique advantage because it taps into the fundamental infrastructure that connects digital identities. Unlike static databases or single-point verification methods, network-based signals provide dynamic, real-time insights that can detect anomalies and confirm legitimate users with unprecedented accuracy.

Through SIM-based authentication, location intelligence, and device insights, mobile networks provide robust security measures that help verify user identities with high accuracy. Advanced features like frictionless silent authentication ensure a seamless yet secure user experience.

Network data and insights can provide critical signals in real-time to AI-based risk assessment platforms to help them generate a more realistic risk score, creating a comprehensive security framework that can detect and prevent fraudulent activities such as SIM swap fraud, account takeover attempts, and unauthorized access. By incorporating network intelligence into existing verification frameworks, organizations can significantly enhance their fraud detection capabilities while maintaining a seamless user experience.

Did you know that you have easy access to network intelligence through Nokia Network as Code ?

The wealth of information within the network available to verify and secure digital identity and detect potential fraud is now easily accessible to financial service institutions, e-commerce merchants, and application providers through an evolved collection of network APIs.

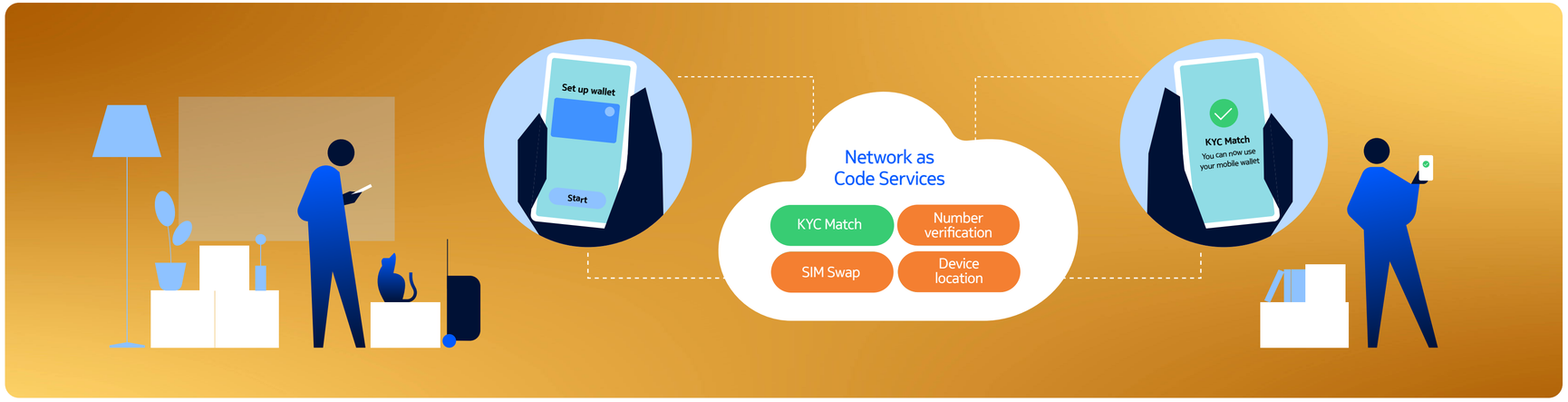
Nokia is empowering digital ecosystems to verify and secure digital identities and combat fraud with an extensive suite of developer-friendly network APIs available through Nokia's Network as Code platform with developer portal.

Aligned to global standardization initiatives like GSMA Open Gateway Initiative (OGI) and Linux Foundation's CAMARA project, Network as Code APIs offer unified API access to real-time digital verification insights and signals across global networks.

Network as Code : Fraud and identity verification API library

- Location verification and geofencing
- KYC verification/ match
- SIM swap
- Call forwarding signal
- Number verification

Enhance your digital KYC processes and streamline onboarding



Digital Know Your Customer (KYC) processes have revolutionized the onboarding of new customers by leveraging advanced technologies to streamline and secure identity verification. Digital KYC involves the use of online platforms and tools such as biometric authentication, document verification, and real-time data analytics to verify the identity of customers quickly and accurately.

By 2025, it is estimated that the global market for digital KYC solutions will reach $1.2 billion, reflecting the growing adoption of these technologies across various industries.

Don’t reinvent the wheel

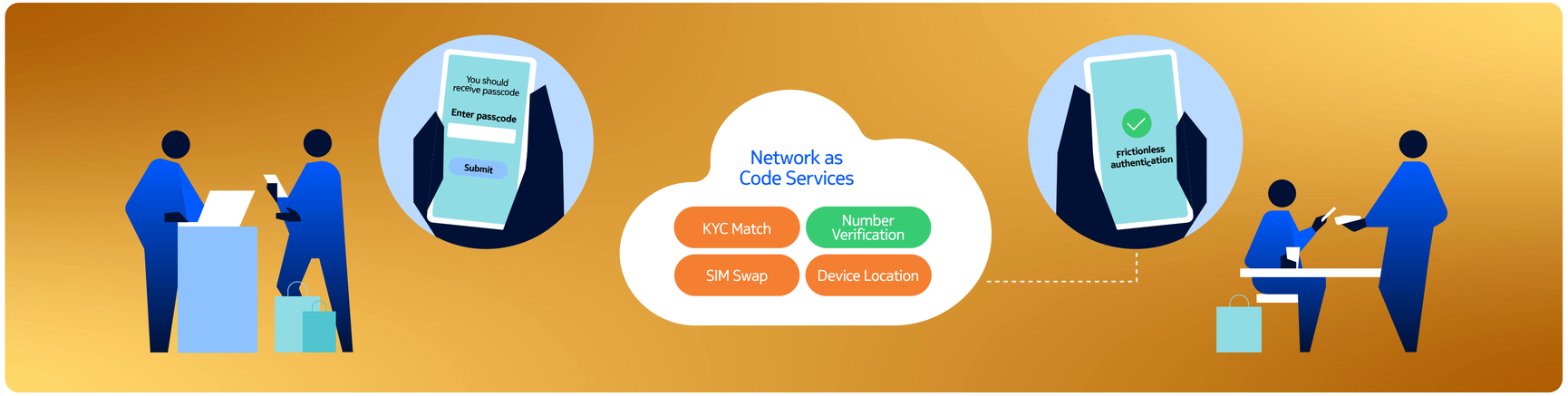
Many solution providers offer APIs (Application Programming Interfaces) to streamline the digital KYC data collection process. However, working with multiple APIs and solution providers can introduce significant cost and complexity. Integrating various APIs requires substantial development resources and careful oversight to ensure compatibility and compliance with regulatory standards.

Wouldn’t it be great if there was one provider who already conducted the due diligence across various data sources for all customers and extended this through a single API to your customer verification systems?

The KYC Match API revolutionizes digital KYC processes by offering enterprises a more efficient, reliable, and cost-effective solution for digital identity verification through mobile network data. This API enables businesses to perform real-time verification by matching customer-provided information against authenticated mobile subscriber data, eliminating the need for multiple API integrations from different providers.

When a customer initiates a verification request, the API compares the submitted information (such as name, ID number, or address) with the telecom operator’s verified subscriber database, providing a simple match/no-match response. This streamlined approach significantly reduces integration complexity, development costs, and maintenance overhead while ensuring high security standards and regulatory compliance. The standardized API also ensures consistency across different operators and markets, making it easier for businesses to scale their KYC verification processes globally.

Expand multi-factor authentication for digital identity verification without the friction



Multi-factor authentication(MFA) is crucial for securing banking and e-commerce transactions in our digital economy. As cyber threats evolve, relying solely on passwords is inadequate to protect sensitive financial information and prevent fraud. MFA adds additional security layers by requiring users to verify their identity through multiple methods. These aim to derive authenticity of a user by querying :

- Something you know : Pin, Password
- Something you have : Trusted device, physical hardware token
- Something you are : Biometrics

While SMS OTP (One-Time Password) is widely used as a second authentication factor (2FA), it creates notable friction in the customer journey. Users must wait to receive the SMS, manually read the code, and input it within a time limit. This process can be frustrating, especially when messages are delayed, network coverage is poor, or users are traveling internationally. Failed or delayed authentications often lead to transaction abandonment and reduced customer satisfaction.

A better solution for trusted device authentication than SMS 2FA

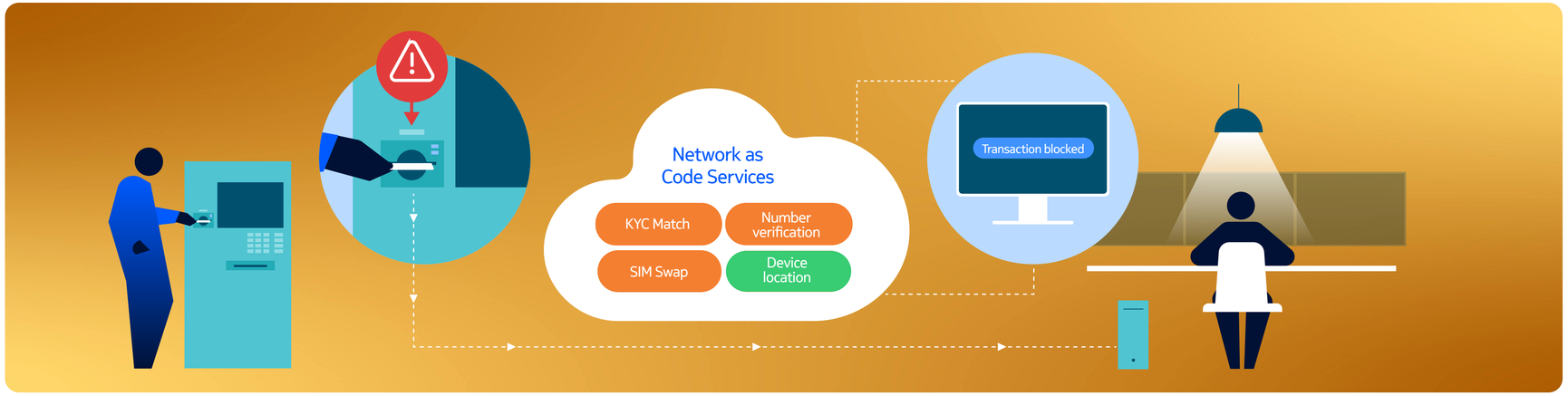
Network-based number verification offers a more elegant solution by leveraging mobile network operator capabilities. This approach authenticates users silently in the background by verifying if the transaction is being performed from the user's registered mobile number. The process happens seamlessly without any user intervention - no codes to type, no SMS to wait for.

The Number Verification API enables businesses and application providers to identify whether a registered user is logging in from a trusted device without relying on SMS based OTP codes. When a user logs in using password credentials, the API queries the network to confirm the transaction is happening from a known device. Based on the returned positive network response, the user is instantly authenticated into the application.

The Number Verification API can be used in conjunction with SIM Swap API and Device Location API to easily bring additional layers of trust to the authentication mechanism.

This frictionless approach maintains robust security while significantly improving the user experience. It reduces transaction abandonment rates, speeds up authentication, and provides a more reliable verification method that works across different scenarios and locations.

Identify and prevent potential card skimming fraud



Card skimming fraud is a type of financial crime where criminals use small devices, known as skimmers, to steal credit or debit card information during legitimate transactions. These devices are often placed on ATMs, gas station pumps, or point-of-sale terminals, capturing card details and PIN numbers without the cardholder's knowledge. The stolen information is then used to create counterfeit cards or make unauthorized transactions.

The global market estimation of losses due to card skimming fraud is substantial, with industry reports suggesting that it costs financial institutions and consumers billions of dollars annually. According to the Nilson Report, card fraud losses worldwide reached $33.8 billion in 2023, with card skimming contributing significantly to these figures. This highlights the critical need for enhanced security measures and consumer awareness to combat this pervasive threat. (Source: Nilson Report, 2023)

Trusted real time location verification can help identify potential counterfeit card transactions

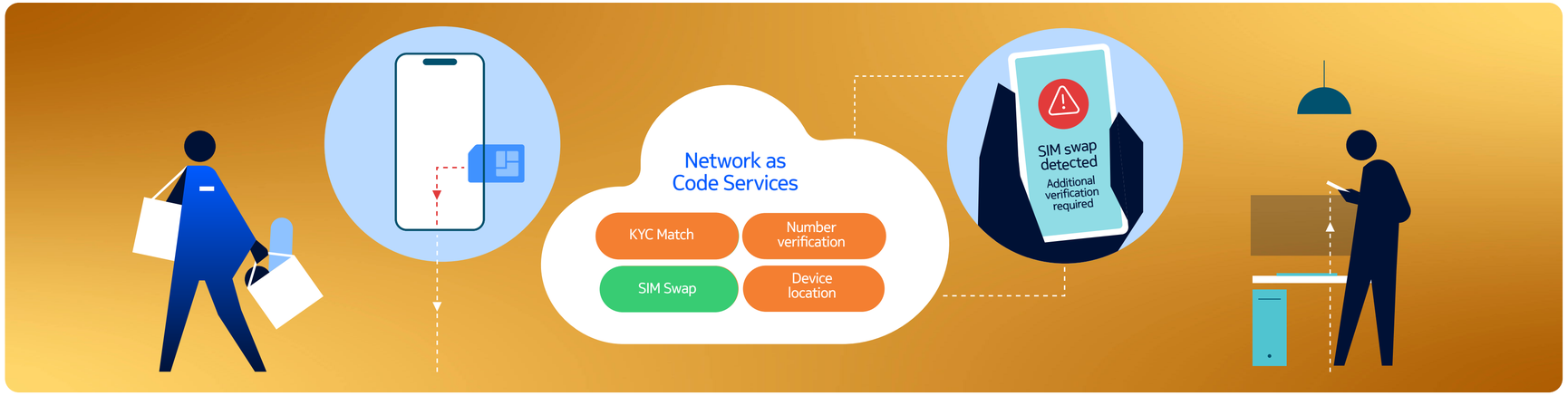
This provides an additional layer of authentication that helps identify potential counterfeit activities. By leveraging network geolocation data, financial institutions can verify whether the location of a card transaction aligns with the cardholder's knownwhereabouts. For instance, if a transaction is attempted in a location far from where the cardholder's mobile device is detected, this discrepancy can trigger an alert for potential fraud.

The Location Verification API simplifies access to trusted device location information enabling banks and payment processors to quickly identify and block suspicious transactions before they are completed, reducing the risk of financial loss and protecting consumers from fraud.

Trusted location verification is not limited to physical card fraud – the same capability can be applied to detect unusual online transactions occurring from a location different from that of the actual user. Accessing user location from the network also addresses the spoofing challenges associated with device GPS location or device IP based location retrieval

Furthermore, real-time location verification can be integrated with other security measures, such as biometric authentication and machine learning algorithms, to create a robust, multi-layered defense against counterfeit card transactions.

Prevent account-takeover attacks through SIM-swap fraud



Mobile phone numbers are the cornerstone of digital identity verification, serving as a trusted identifier for authentication across banking, e-commerce, social media, and online services. This heavy reliance on phone numbers for account security has made them an attractive target for cybercriminals and fraudsters who are taking advantage of social engineering to swap out SIMs without the knowledge of the consumer.

Once the SIM has been swapped, SMS OTPs designed to be delivered to the consumer are now redirected to the fraudster's device which has the new SIM with trusted credentials. Through this approach, a full account takeover (ATO) can be initiated, resulting in heavy financial losses for the end user.

In February 2020, a SIM Swap attack in North America enabled fraudsters to access a cryptocurrency account resulting in the loss of nearly 1500 Bitcoin and approximately 60,000 Bitcoin cash. Depending on country regulations, the onus is often on the bank or the merchant to reimburse the loss to the consumer.

How do you identify if a SIM has been swapped before authorizing a transaction ?

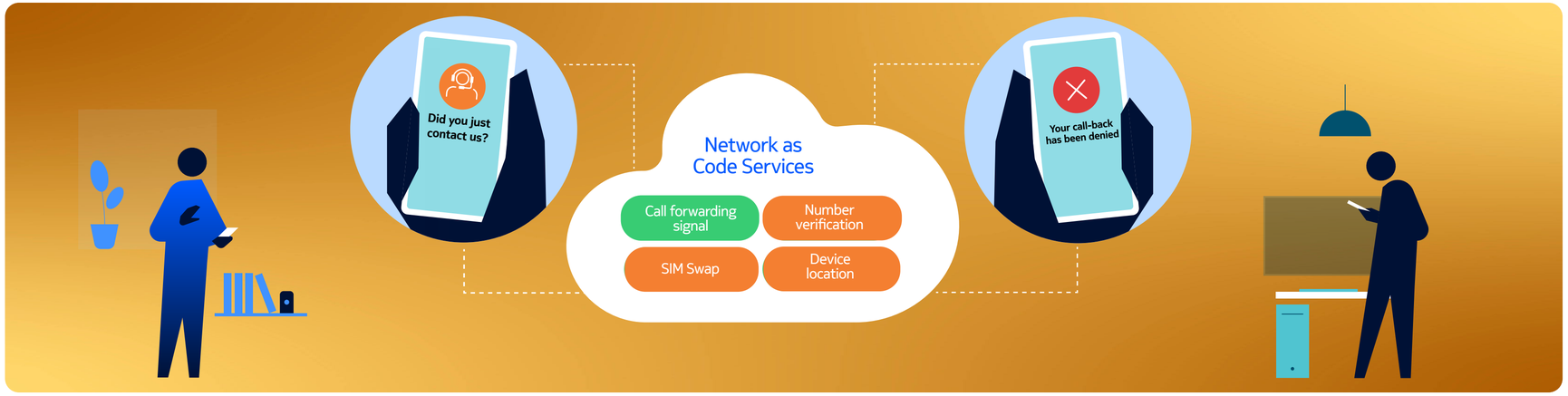
SIM swap attacks can have disastrous consequences – thus it is essential that banks and merchants take advantage of available risk signals before authorizing a transaction. Information about SIM changes is available on Mobile Network Operators (MNO) databases, and this is now accessible through a globally standardized SIM Swap API.

The SIM Swap API monitors and detects real-time changes to the mobile device's SIM card. It adds an additional layer of security to SIM-based authentication methods, such as SMS and OTPs, to alleviate the risk of account takeover fraud.

It becomes essential when fraudulent transactions utilize SIM-swapping techniques to intercept SMS messages, enabling fraudsters to reset passwords or obtain verification codes to gain unauthorized access to secured accounts.

For example, when a bank receives a request for SMS-based 2FA, it can request the SIM Swap API to check how recently the SIM card has been changed. If the phone number is associated with a newly provisioned SIM card or has been ported to a different carrier, the bank will receive this information from the API, helping it temporarily block transactions until the user can confirm their identity.

Secure customer support from impersonation fraud



Fraudsters are uncovering newer methods of digital identity theft and impersonation and one of the potential vulnerability points is customer support.

First, call forwarding is activated by the fraudster so that calls for the registered customer are diverted to the fraudster's device. A request for call-back from application support is initiated online. When the customer support team calls the genuine customer's number, this call is forwarded and now received by the fraudster.

Using personal identity information of the victim sourced through phishing, social media and data available on the dark web, the fraudster passes all the identification checks initiated by customer support and then proceeds to carry out account transactions by beguiling the customer representative.

In this case, the risk is firmly with the bank or merchant who has vetted and supported the transaction through their customer support. Thus, it is essential to identify if genuine customers have call forwarding activated for their number before contacting them.

Identify the risk signals of Call forwarding prior to customer support engagement

Leveraging the Call Forwarding Signal API, banks and merchants can carry out an additional check to identify if a customer's call is being forwarded to an unknown device. While this could have been genuinely initiated by the end customer, a zero-trust approach should activate further verification steps before customer support initiates a call-back and carries out account transactions on the customer's behalf.

The Call Forwarding Signal API helps banks detect fraud by verifying if a customer's phone has "unconditional call forwarding" activated. This prevents fraudsters from intercepting calls intended for customers by redirecting them to the numbers they control. Banks use this API to check the call forwarding status on a customer's phone number, allowing them to take appropriate action if necessary.

The attack scenario occurs when a fraudster gains unauthorized access to a customer's phone and activates call forwarding to their number to bypass security alerts, perform transactions, or alter account settings without the customer's knowledge.

The bank can detect this fraud attack using the Call Forwarding Signal API to check the phone's status. If the call forwarding to an unrecognized number is detected, the bank blocks or delays the transaction and securely notifies the customer, preventing fraud and safeguarding their account.

ABI Research ranks Nokia overall leader and top innovator for telco API platforms

Nokia Network as Code

The industry's leading network API platform designed for enterprise business-critical needs

Nokia Network as Code is the industry's leading API platform that enables you to easily integrate specialized capabilities and rich insights from the network into your digital identity verification and fraud management solutions.

Since launching the Network as Code platform in late 2023, Nokia's ecosystem of 50+ Network as Code partners covers leading global networks including BT, Orange, Telefonica, Vodafone and US Majors.

Nokia's commitment to widespread API adoption extends beyond network-side aggregation -our ecosystem also includes hyperscalers like Google Cloud; Communications Platform as a Service (CPaaS) providers such as Infobip; large system integrators such as Global Logic and Wavemaker; vertical independent software vendors like Elmo; and the world's largest public API hub through Nokia's acquisition of Rapid.

Unified API access across global networks

You don't need to update your codebase for every region and service provider. Network as Code offers an expanded set of Network APIs with unified API access across all leading global networks, greatly simplifying development complexity.

Take advantage of extreme API performance and availability

Powered by best-in-class API hub technology from Rapid (now acquired by Nokia), Network as Code offers you guaranteed API performance and the highest API availability across the industry.

Our API technology has been reliably proven to execute in excess of 63 billion API transactions annually and is trusted by leading enterprises across the financial services, aviation, automotive, fleet, and telecommunications sectors.

You don't need to be a network expert

Designed 'developer-first' with a comprehensive developer portal, sandbox environment and GenAI based code generation assistant, Network as Code makes it easy to embed network data, insights and specialized capabilities into your application without needing you to interpret complex telecom parameters and data sources.

Flexible billing and charging models to suit your business needs

Whether you're a startup or a global enterprise, you can scale your API usage effortlessly with our transparent pricing. Our pay-as-you-go model means you only pay for the API calls you actually make—ideal for keeping costs low during early development or small-scale deployments. And when your needs grow, you can upgrade to a tiered subscription with customizable packages that fit your exact requirements.

Get started with Nokia Network as Code

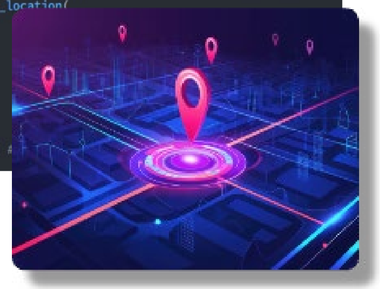
```python
import network_as_code as nac

from network_as_code.models.device import DeviceIpv4Addr

# We initialize the client object with your application key
client = nac.NetworkAsCodeClient(
    token="<your-application-key-here>"
)

# Create a device object for the mobile device we want to use
my_device = client.devices.get(
    # The phone number does not accept spaces or parentheses
    phone_number="+36721601234567"
)

# For estimations, use the is_there object
# followed by the `verify_location()` method
# with the geo-coordinates and maximum age in seconds.
# If the amount in seconds is not given, the default will be 60 seconds.
result = my_device.verify_location(
    longitude=60.252,
    latitude=25.227,
    radius=10_000,
    max_age=3600
)
print(result.result_type) #
```

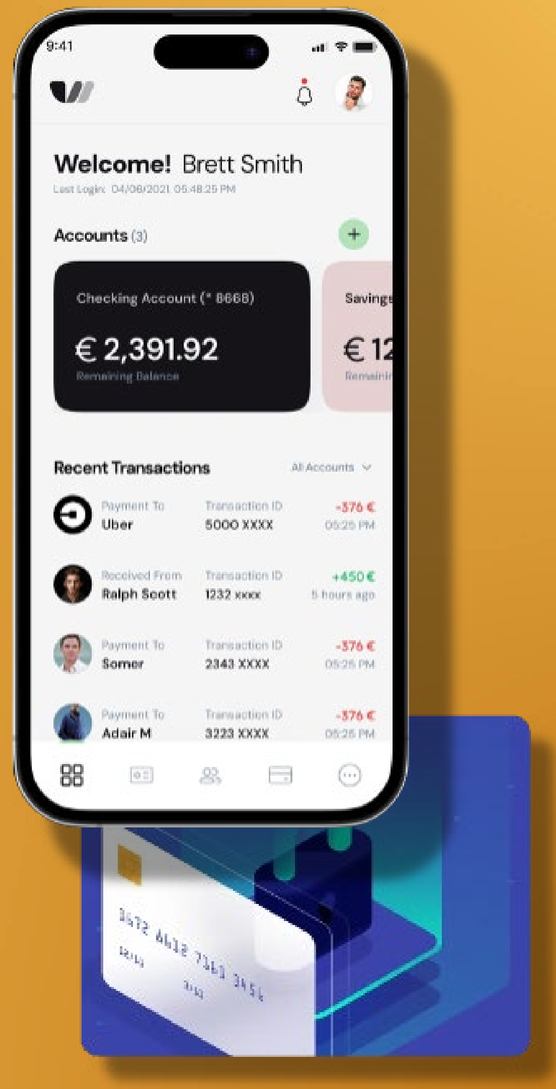


Quickly build ready-to-deploy use cases on our developer portal

- Comprehensive documentation, tutorials and sample code for every Network as Code API
- Google Gemini GenAI code generation assistant simplifies use case development for first time adopters
- Full featured sandbox environment to help you test and evaluate use cases across every network

Accelerate development with prefabs from Nokia and our partners

- Fully customizable consumer-grade UX
- Prefabs embedded with enterprise-class security
- Code and Ops freedom for extensive scalability
- Embeddable web components for third-party applications



Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214792

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.