2024

Leveraging Mobile Network APIs for Fraud Prevention in the Canadian Market

White Paper

Contents

Introduction

In an increasingly digitized world, fraudulent activities around digital accounts have become more prevalent and sophisticated.

As technology evolves, so do the methods employed by fraudsters to gain unauthorized access to personal and financial information. Recognizing the critical need for robust tools, mobile carriers work with enterprises and independent software vendors (ISVs) to act as a source of truth for account creation and access through mobile network APIs. **EnStream**, a joint venture of Canada's largest mobile carriers Rogers, Bell, and Telus, has been at the forefront of providing mobile network APIs to combat digital account fraud. Through the seamless integration of these APIs, Canadian enterprises have been able to protect customer privacy and mitigate the risks associated with fraudulent activities.

This white paper explores the role of mobile network APIs in addressing digital account fraud, highlighting their value proposition, use cases, and the impact they have on the Canadian market.

Understanding Digital Account Fraud

Digital account fraud encompasses a wide range of activities conducted within online platforms. It refers to the unauthorized access, manipulation, or exploitation of digital accounts belonging to individuals or organizations for fraudulent purposes. These accounts can include but are not limited to:

Financial Accounts : Such as bank accounts, credit card accounts, investment accounts, and digital wallets.

Online Shopping Accounts : Accounts on e-commerce platforms like Amazon, eBay, or any other online retailer where financial information may be stored.

Social Media Accounts : Platforms like Facebook, X, Instagram, or LinkedIn where personal information and sometimes financial information may be stored.

Email Accounts : Email addresses associated with personal or business use, which may contain sensitive information and serve as a gateway to other accounts.

Subscription Services : Accounts for streaming services like Netflix or Spotify, or other subscription-based platforms.

Digital Account Fraud Can Take Various Forms

Identity Theft : Fraudsters may use stolen personal information to create new accounts or take over existing ones, impersonating the legitimate account holder to carry out fraudulent activities.

Phishing and Social Engineering : Fraudsters use deceptive techniques, such as fake emails, messages, or phone calls, to trick individuals into divulging sensitive information like login credentials or financial details.

Number Porting : also known as mobile number portability (MNP), is a legitimate process that allows mobile phone users to transfer their phone number from one carrier to another without changing their phone number. This process is typically used when a customer switches from one mobile carrier to another while retaining the same phone number. However, in the context of fraud, number porting is exploited by fraudsters to gain unauthorized control of a victim's mobile phone number. The fraudster convinces the victim's mobile carrier to transfer the victim's phone number to a different carrier onto a SIM card under the fraudster's control. Once the number is successfully ported, the fraudster can intercept calls, text messages, and authentication codes intended for the victim, effectively taking over the victim's mobile communications.

SIM Swapping : also known as SIM hijacking, is another fraudulent tactic used to gain unauthorized control of a victim's mobile phone number. In a SIM swapping attack, the fraudster convinces the victim's mobile carrier to deactivate the victim's SIM card and activate a new SIM card under the fraudster's control. This allows the fraudster to receive calls, text messages, and authentication codes intended for the victim on the new SIM card. Unlike number porting, which involves transferring the victim's phone number to a different carrier, SIM swapping typically involves deactivating the victim's existing SIM card and activating a new SIM card on the same carrier.

Multiple Number Use : The use of a disposable or temporary mobile numbers to commit scams or illicit activities and avoid detection.

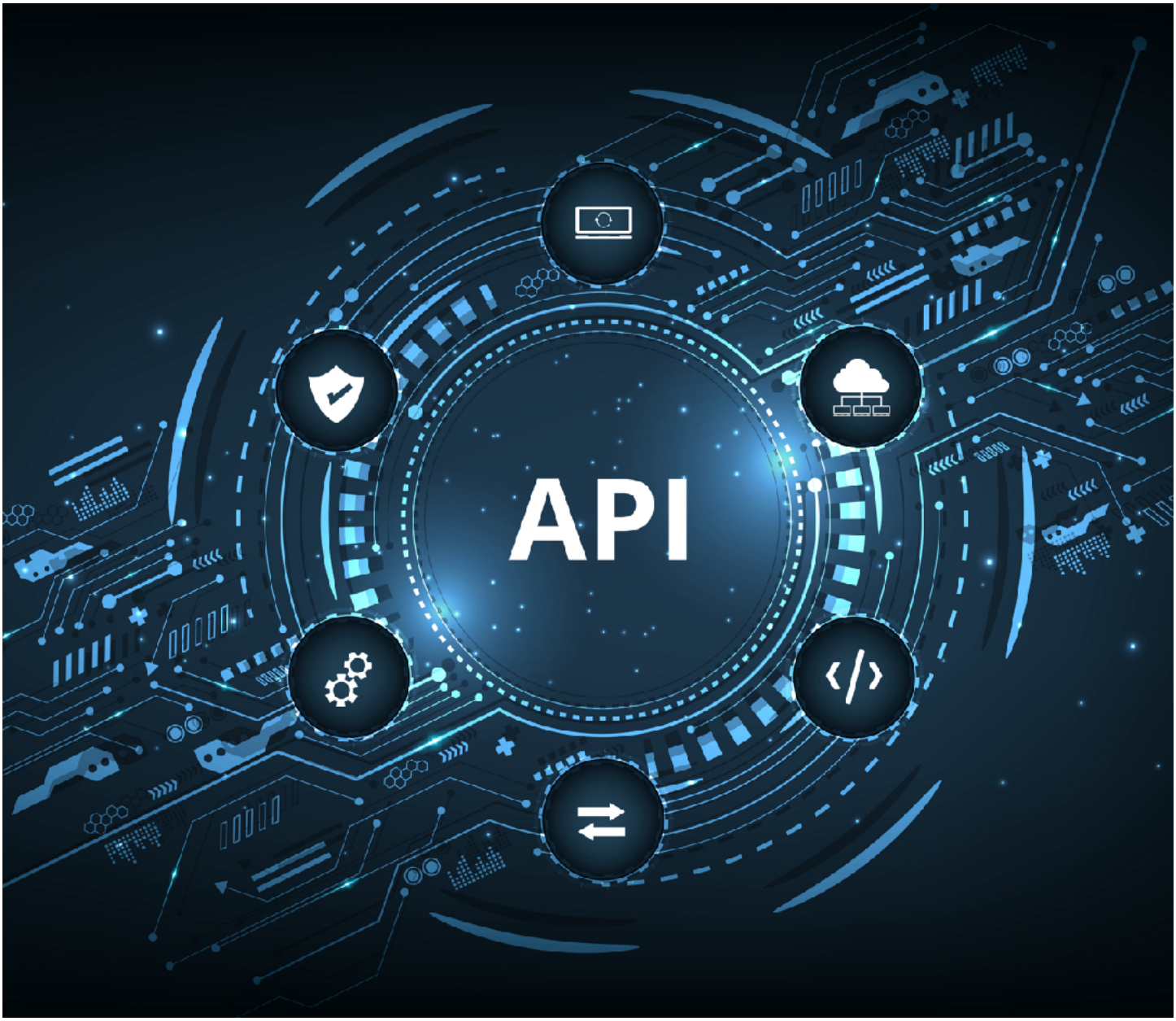
Account Takeover : Where fraudsters gain unauthorized access to an individual's or organization's account by stealing login credentials through various means such as phishing scams, data breaches, SIM swapping, etc. Once inside, they may conduct unauthorized transactions, change contact information, or exploit the account for further fraudulent activities.

Payment Fraud : This involves unauthorized transactions using stolen payment information stored in digital accounts, such as credit card numbers or bank account details. Fraudsters may make purchases or transfer funds without the account owner's consent.

Fraudulent Applications : Fraudsters may submit fraudulent applications for new accounts, such as credit cards or loans, using stolen personal information. They then exploit these accounts for financial gain.

These fraudulent activities pose significant risks to both individuals and businesses, leading to financial losses, reputational damage, and legal liabilities. To combat digital account fraud, individuals and organizations use various tools, including multi-factor authentication, encryption, fraud detection algorithms, and user education to recognize and avoid phishing attempts and other fraudulent tactics. Financial institutions and other online service providers may additionally monitor accounts for suspicious activity and implement fraud prevention measures such as transaction alerts and account freezes.

However, the evolving nature of fraud requires continuous innovation and adaptation. This is where mobile network APIs can provide solutions.



The Role of Mobile Network APIs in Fraud Prevention

Mobile network APIs play a crucial role in fraud prevention by leveraging real-time data from mobile networks to verify user identities, authenticate transactions, and detect suspicious activities. These APIs enable seamless integration between digital platforms and mobile carriers, allowing businesses to validate valuable information such as device identifiers, location data, and subscriber profiles. By analyzing this data in real-time, businesses can identify anomalies, detect fraudulent activities, and take proactive measures to mitigate risks.

Consent Flows and User Privacy

It's essential to emphasize that mobile network APIs operate within strict consent flows established by users. Mobile carriers do not share Personally Identifiable Information (PII) or put PII at risk. Instead, they ensure that user consent is obtained and respected throughout the authentication process, safeguarding user privacy while combating fraud effectively.

Use Cases – How Mobile Network APIs Address Digital Account Fraud

Mobile carriers have a wealth of information to verify that people are real in the digital world. Through device-centric, location-centric and identification-based information, mobile network APIs are able to authenticate account access.

Device-centric information refers to the information related to a mobile device.

Location-centric information refers to device location.

Identification-based information refers to the data for identifying individuals. This may include personal information such as name, address, or date of birth.

Account access can be authenticated at onboarding or at account login, the information the mobile network APIs check, differs based on the use case. This section will examine where a fraudulent activity commonly occurs, and the information mobile network APIs access, based on the use case to mitigate risks.

Account Onboarding

During the account onboarding process network APIs serve as a vital defense against fraudulent activities. Consider a scenario where a fraudster tries to exploit stolen identity information to create an account. While they might possess accurate details such as a legitimate phone number and name, discrepancies like an incorrect date of birth could raise suspicions. Here, network APIs come into play with ***identification-based information***. Typically in under 2 seconds, they conduct a thorough check against mobile records to verify the user's information. If any inconsistencies are detected, mismatches between provided data and authenticated records, the API promptly denies the account creation attempt, preventing potentially fraudulent activity.

Account Access

Mobile applications often rely on phone numbers as a means of identity verification during the user authentication process, typically through the use of SMS One-Time Passwords (OTPs). While effective in confirming that the user is the rightful owner of the mobile device associated with the provided phone number, this method can disrupt the user experience by requiring manual interaction with the SMS message, thus interrupting the user's flow and navigation within the application. With the use of a mobile network API, mobile applications can offer a more seamless and user-friendly onboarding experience, enabling the application to request reliable and frictionless authentication without requiring direct interaction from the user. Instead of sending an SMS OTP, the application can initiate a verification process through a Number Verification API, which verifies the possession of the phone number associated with the user's account in real-time.

Companies may choose to further reduce risks by using mobile network APIs to pull ***mobile device-centric information*** to detect any changes to a device that may indicate fraud such as number porting, SIM swap, and account tenure. These fraudulent tactics underscore the importance of robust tools and vigilant monitoring to detect and prevent unauthorized account access.

Monitoring

Continuous monitoring of user activities is essential for detecting and preventing fraudulent transactions. Mobile network APIs provide businesses with access to valuable data from mobile carriers, including device identifiers, location data, and usage patterns, enabling them to identify suspicious schemes as they develop.

Overall, the monitoring use case demonstrates the importance of continuous surveillance and proactive intervention in detecting and mitigating fraudulent activities in real-time. By leveraging mobile network APIs for monitoring purposes, businesses can enhance their fraud prevention efforts and protect themselves and their customers from financial losses and reputational harm.

Industry Focused Use Cases

Financial Institution

Many leading Canadian banks utilize mobile network APIs to strengthen fraud protection of their application processes by verifying the identity of the subscriber, or by leveraging device/SIM changes to check for signs of unauthorized mobile account takeover. Traditionally, financial institutions rely on static information provided by applicants, such as addresses and identification documents, to authenticate their identities and assess the risk associated with new account applications. However, these methods may be susceptible to fraud, especially in cases where applicants provide falsified or stolen information.

By leveraging mobile network APIs, the bank can implement a more robust and dynamic authentication mechanism. When an applicant submits an account application, the bank's systems can initiate a request through the mobile network API, which retrieves real-time data about the mobile account and any recent suspicious activity. This information provides valuable context and additional layers of verification, enabling the bank to detect potential instances of fraudulent activity.

E-commerce Platform

A popular e-commerce platform in Canada leverages mobile network APIs to strengthen authentication and prevent account takeover. By analyzing device identifiers from mobile carriers, the platform is able to identify suspicious login attempts and prompt users to verify their identity through tools, such as biometric authentication or one-time passwords. This proactive approach to fraud prevention not only protects the platform's users from unauthorized access but also enhances the overall security posture of the platform.

Credit Card Issuer

A credit card issuer harnesses mobile network APIs to reduce fraud risk and enhance the efficiency of its credit card application process, ensuring the integrity of the identity verification process and proactively mitigating the risk of fraudulent activities.

When an individual submits a credit card application, the APIs are leveraged to authenticate the applicant's identity by cross-referencing the provided personal information, such as name, address, and date of birth, against identification-based information. This real-time verification process helps ensure that the applicant is who they claim to be, minimizing the risk of identity theft and fraudulent applications.

Benefits and Impact

The implementation of mobile network APIs for fraud prevention has yielded measurable benefits for businesses across various industries in Canada. Key metrics and impact include :

Reduction in fraudulent account creations. Businesses using mobile network APIs for account onboarding have reported a significant decrease in fraudulent applications, resulting in cost savings and improved operational efficiency.

Decrease in account takeover incidents. By strengthening authentication and monitoring user activities, businesses have seen a decline in account takeover incidents, reducing financial losses and mitigating reputational risks.

Improved customer experience. Tools, such as multi-factor authentication and real-time fraud detection, have bolstered customer trust and satisfaction, leading to increased loyalty and retention rates.

Other Opportunities

Beyond fraud detection, mobile network APIs offer a myriad of opportunities to innovate and enhance an ISVs offering, enabling a more personalized and seamless customer experience. Here are some additional ways mobile network APIs can be leveraged.

Quality of Service Monitoring

Mobile network APIs offer insights into network connectivity and performance metrics, allowing ISVs to monitor the quality of service (QoS) experienced by their users. For example, a video streaming service can use mobile network APIs to detect fluctuations in network bandwidth and adjust video quality dynamically to ensure uninterrupted playback for users. Similarly, online gaming platforms can optimize gameplay experiences by prioritizing low-latency connections and reducing network congestion.

IoT Device Management

With the proliferation of Internet of Things (IoT) devices, mobile network APIs play a crucial role in managing and monitoring connected devices remotely. ISVs can use mobile network APIs to provision, configure, and troubleshoot IoT devices, ensuring seamless connectivity and optimal performance.

By exploring these additional opportunities beyond fraud services, ISVs can unlock new possibilities for innovation and differentiation, enabling them to stay ahead in today's competitive marketplace while delivering exceptional value to their customers.

Accessing Mobile Network APIs

GSMA, an organization that represents mobile carriers worldwide, announced the **Open Gateway initiative** in 2023 to standardize mobile network APIs across carriers globally.

Prior to this initiative, lack of interoperability among carriers on a global scale made mobile network APIs difficult to implement.

Canada has been a leader in the mobile network API market via **EnStream**, which acts as a mobile signal aggregator for the country's mobile networks, offering a one stop integration point for Canadian mobile network APIs. The GSMA Open Gateway initiative will further enable ISVs of all sizes to integrate mobile network APIs into their software. In the near future, global marketplaces will have a key role in providing access to GSMA's standardized mobile network APIs by aggregating them across all countries, including Canada, and allowing developers to consume them via a single global endpoint.

EnStream in collaboration with their partner networks Rogers, Bell and Telus, plan to accelerate digitization and take advantage of 5G-enabled solutions for enterprise and small and medium business customers. Our objective is to launch a range of antifraud-based mobile network APIs via hyperscalers as of 2025.

In addition, Rogers and Microsoft have established a five-year strategic alliance to accelerate digitization and take advantage of 5G-enabled solutions using **Microsoft Azure Programmable Connectivity (APC)** for enterprise and small and medium business customers. Available to ISVs in Canada and around the globe, APC is a cloud-based platform that enables developers to access and integrate network API capabilities into their applications and services. By using APC APIs, developers will be able to provide additional security and protection for their customers, such as detecting and preventing fraudulent calls, messages, and transactions.

Conclusion

Digital account fraud presents substantial risks to individuals and businesses, resulting in financial and reputational harm.

To counter these threats ISVs utilize various tools, but ongoing innovation is essential due to fraud's evolving nature. Mobile network APIs offer solutions by enabling adaptable and innovative anti-fraud strategies, as proven over decades by EnStream for Canadian enterprises. With the launch of GSMA Open Gateway for standardized mobile network APIs and global API marketplaces to aggregate APIs across carriers worldwide; ISVs worldwide will soon leverage mobile network APIs for simplified, interoperable solutions on a global scale.

For more information :

EnStream LP
55 University Avenue, Suite 903
Toronto, Ontario M5J 2H7
Canada

T +1.416.365.9000
@ info@enstream.com
W www.enstream.com