Stopping SIM SWAP in Its Tracks

With the growth and sophistication of mobile banking, a new security vulnerability has become the smartphone. Fraudsters have shifting their focus from desktop-based fraud to mobile attacks.

Fraudsters view the mobile is the new "weakest link" and have created creative and sophisticated mobile fraud attacks that have swindled millions and caused considerable damage to financial institutions.

The new financial fraud kid-on the-block is SIM swap. At its most basic level, a SIM SWAP is when a fraudster persuades a mobile carrier to switch your phone number over to a SIM card they own. Bad-guys are not doing it to hoax you or to rack-up long-distance charges... they are doing it to amass big bucks by diverting your incoming messages, to easily over-ride text-based authentication that protects your most sensitive accounts.

Paygilant Differentiators

- **HIGHEST LEVEL FRAUD PROTECTION**
  Accurately distinguishes between legitimate and deceitful transactions, stopping mobile fraud in its tracks.

- **TRUE FRICTIONLESS EXPERIENCE**
  Enables an interruption-free transaction experience.

- **NO PRIVACY CONCERNS**
  Ensures that customers' private and personal data cannot be compromised. Paygilant uses a hybrid architecture that generates an authentication decision safeguarding sensitive data.

Legacy Authentication Solutions Struglle to Stop SIM SWAP

Legacy authentication technologies validate transactions anomalies and device authenticity, not actual end-users. One-time password verification was not designed to identify and stop malicious activity that compromise smartphones, not to mention that the OTP is transmitted to the fraudster's device. Only by integrating the user's unique bio markers, along with his/her device fingerprint data and transaction analysis can organizations curb SIM SWAP.

Paygilant's Contextual Multi-dimensional Authentication is designed to fight SIM SWAP attacks. Paygilant's continuous authentication of users based on unique and nearly impossible to copy personal behavior patterns allows organizations to confront the threat of SIM SWAP.

How Does Paygilant Stop SIM SWAP During The Users Journy

Paygilant's six intelligence sets work as layers to stop SIM SWAP throughout the different stages of the user's journey.

	App Download	Onboarding/ registration	New card enrollment	On-going transactions
Users Journey	1	2	3	4
Paygilant's six intelligence sets				
How Paygilant helps stop SIM SWAP	Paygilant analyses the device environment (contacts, pics, cellular & Wi-Fi networks activity, etc.) to determine if device is suspect and likelihood of SIM SWAP.	Looks at the activity on a specific device to determine if multiple SIM's have been used on it? If multiple SIMs have been used on same device, then likelihood of SIM SWAP is high	Checks if multiple devices / enrolled cards have used the same SIM. If determined that indeed the SIM was used on several smartphones, then a high likelihood of SIM SWAP is indicated and flagged.	Analyzes and correlates transaction-based data such as customer spending habits, transaction location, time of payment, etc. to determine likelihood of SIM