paygilant

Fraudless. Frictionless. Effortless.

Solution Overview

White paper

paygilant.com

Introduction

The mobile banking and payments markets are growing at an exponential rate, as consumers and merchants alike are adopting new financial, eCommerce and digital wallet payment methods. With mobile banking and payments becoming mainstream, fraud continues to shift to the mobile channel, threatening this developing ecosystem. The new digital financial market is challenged to raise the security of its money transfer and payment solutions, without compromising a smooth user experience and privacy.

Paygilant's innovative frictionless authentication and fraud prevention solution protects the entire user-journey. Paygilant detects fraudulent transactions from app's initial launch to ongoing transactions, while seamlessly authenticating the legitimate customers. This eliminates the trade-off between preventing fraud and delivering an uncompromised user experience and privacy.

This document showcases Paygilant's fraud prevention and frictionless authentication solution, referring to specific field-based use cases, product architecture and solution benefits.

The Changing Mobile Fraud Landscape

As mobile use grows so does mobile fraud. Fintech banks build their products and services with a mobile first strategy. In addition, new payment solutions are emerging, offering more value to banked and unbanked consumers, in the form of in-store, online, P2P money transfer and mobile wallets. Banks, payment providers and merchants are challenged to secure their applications against various attack MOs:

Transaction Fraud, New Account Fraud, Account Takeover Fraud (ATO) and Cross-Bank Fraud

New Account Fraud is the use of a fake or stolen identity to open a new account. Fraudsters have become experts at stealing personal identities and using them for mobile fraud. Whether fraudsters use the victim's genuine identity, or bits and pieces of real data to create a synthetic identity, the goal remains creating a new online account to commit fraud.

Account Takeover Fraud is a form of identity theft, in which the fraudster gets hold off a victim's credentials and account through a data breach, malware, social engineering or phishing. It is then used to make unauthorized transactions from within the account, liquidating it or using its credit to buy goods or services.

Transaction Fraud occurs when a stolen payment method details or card data are used to generate an unauthorized transaction. The shift to real-time transactions causes significant security challenges for banks, merchants and card issuers alike. Instant payments and money transfers elevate the chances of fraudulent transactions going undetected.

Cross-Bank Fraud comprises a multi-link attack. An ***Account Takeover*** is initiated at bank #1, while the fraudster creates fake accounts at bank #2 (***New Account Fraud***), to liquidate the stolen funds. The funds are then transferred from the external (bank #1) compromised account to the new fake accounts (bank #2) and from there, to the legit account, owned by the fraudster – from which it is liquidated.

Historically banks, eCommerce and digital wallet providers have been pursuing the mitigation of these types of fraud, while absorbing losses written off as a cost of doing business. However, as fraudsters become more sophisticated and the cost of fraud continues to increase, this sense of urgency too is changing.

Paygilant's Mobile Fraud Prevention and Authentication Solution

Paygilant's fraud prevention and frictionless authentication solution is a combination of a lightweight SDK which seamlessly integrates with the application, and a powerful, analytics-based backend risk engine. Using proprietary and unique intelligence sets, Paygilant's solution can decisively identify fraud/no-fraud transactions, with an unparalleled accuracy.

Paygilant's SDK is designed to securely transmit the necessary data points to Paygilant's servers, where the risk score is generated. The entire process occurs in milliseconds where security and user's privacy are kept intact. Paygilant applies end to end security controls and adheres to worldwide privacy policies and guidelines.

Paygilant's Six Intelligence Sets that Authenticate Customers and Prevent Mobile Fraud

By integrating, correlating and analyzing six proprietary fraud intelligence sets, Paygilant determines, whether a mobile based transaction is legitimate or fraudulent. Paygilant analyzes multiple data attributes using dynamic layers which include user behavior, device identification, user transaction and human/machine activity. This is used to weave an identity representation of the mobile user, providing a risk-score that indicates the risk level of each transaction. Paygilant's unique mobile fraud methodology consists of multiple intelligence sets including **App Insights, Bio Markers, Activity Map, User Space, Device DNA and Transaction View.**

Device DNA

Next gen of device fingerprinting. Various attributes observed on the device contribute to forming a unique device ID. Device model, screen, memory, UUID, OS, IP, geolocation, emulation, rooting/jailbreaking are a few of the attributes observed. Paygilant's formula of blending hardware characteristics with device parameters, generate a robust, unique fingerprint for each device. This fingerprint enables identifying legitimate users and serial fraud attacks.

User Space

Intelligent, privacy preserving analysis of the User's Space on the mobile device, provides valuable insights into fraudulent environments. User Space produces an immediate value in hard-to-analyze scenarios such as new account opening, where no prior history about the user or device exists. It also significantly mitigates the friction, by distinguishing between a legitimate user returning from a new device, and an Account Takeover attack, launched from a fraudulent smartphone.

Activity Map

A unique flow of the user's navigation in the app is mapped and profiled. The Activity Map Intelligence Set analyzes the interaction of a user with the mobile application. It determines whether the interactions are consistent with the legitimate user's activity or performed by a fraudster, using compromised credentials, card or identity.

Bio Markers

Paygilant's behavioral biometrics observes bio markers to seamlessly authenticate legit customers and passively identify a fraud activity. Paygilant analyzes various bio attributes that contribute immensely to identifying the user. Such include touch velocity, intervals, size of touch inputs, finger velocity, scrolling pace and drag length, typing biometrics, gestures and more. A combination of all Bio Markers factors creates a unique individual bio profile for each customer and fraudster.

App Insights

As data becomes available to Paygilant by the application, it's utilized for the purpose of validating the identity of the user. This is performed by cross-referencing it with internal and external data sources.

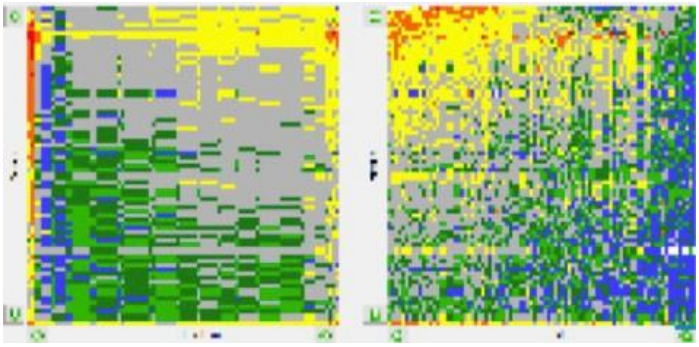
Transaction View

Paygilant employs propriety transaction behavioral maps. The Behavioral Maps represent the financial transactions and spending habits of a specific customer. The maps are created using Paygilant's patented machine learning algorithms. A Behavioral Map represents a clear, high resolution picture of the different risk zones, and is a key factor in determining the risk of a specific transaction. It has the following key characteristics:

- Private Maps: Each map is unique, calculated and maintained on a per-user basis, therefore representing a transaction risk level for each customer's transaction.

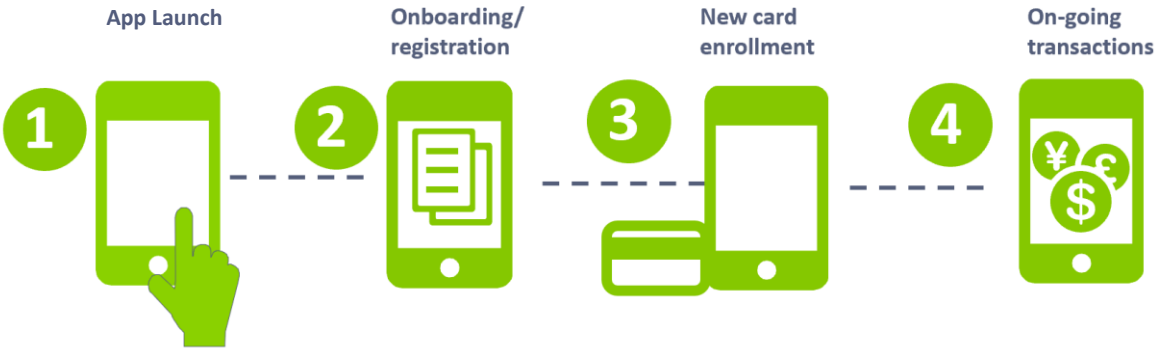
- Public Maps: Each private map is compared with the public behavior, to determine the virtual proximity of the transaction between individuals and their peers.

Paygilant behavioral maps



Fraud Identified at Every Stage of The User's Journey

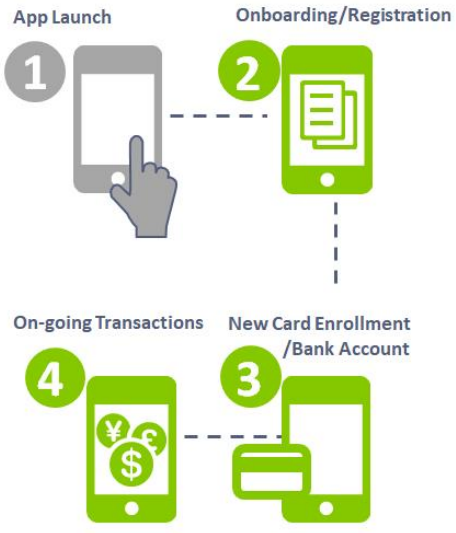
The user's journey is the process that a typical user performs when conducting a financial transaction/payment. The course of action includes the following steps:



It is the precise weave and cumulative build of the six Intelligence Sets, that makes up Paygilant's secret sauce. Paygilant's Intelligence Sets are dynamic layers which are activated throughout the different stages of the user's journey.

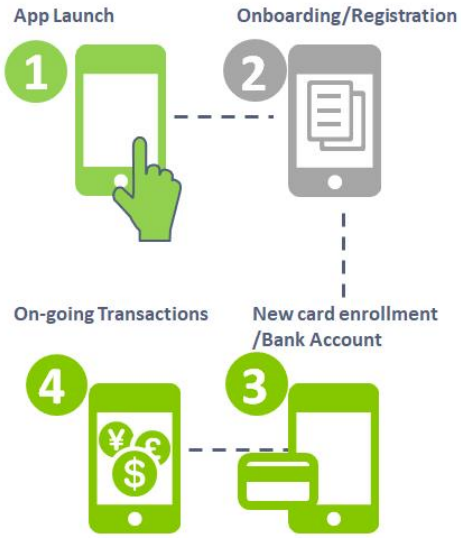
App Launch (Stage 1)

Once the App has been downloaded and launched, Paygilant User Space and Device DNA are triggered. Initial analysis based on respective data points, characterize a stolen device or a swapped SIM. Paygilant's detection from day-1 comes into play by indicating on any non-human and non-user fraudulent activities related to emulators, bots and compromised devices. Paygilant red flags the potential threat from the moment the app has been initially launched.



Onboarding/Registration (Stage 2)

Account opening is highly susceptible to fraud attacks. During onboarding, Paygilant's Device DNA, User Space, Activity Map and Bio Markers are activated, indicating a legit or fraudulent account creation. eKYC processes are enriched with unique and valuable inputs from Paygilant to determine, whether an account is opened by a legit user or a fraudster.



New Card Enrollment/Bank Account (Stage 3)

In cases where the app enables in-store or online payments, Paygilant activates its Card Enrollment checkpoint. The combination of 5 Intelligence Sets, point on abnormal activities related to debit/credit card on the app. Paygilant accurately distinguishes between normal user's card enrolment vs. fraudulent one. It's the combined attributes of the Intelligence Sets that provide a trustworthy risk assessment.

On-going Transactions (Stage 4)

The transaction phase triggers all six Paygilant's Intelligence Sets, indicating on an authenticated user or a risk of fraud.

Summary

Paygilant's unique mobile 1st approach, integrates and correlates multiple Intelligence Sets which accurately detect fraud and enable a frictionless user experience - from app launch, to on-going transactions. Without impacting and imposing on the user, Paygilant operates in the background of the app to seamlessly alert on a suspicious transaction before it occurs.

Paygilant's ability to provide ongoing and continuous data-analysis, reduces the use of any step-up authentication (Pincodes, passwords, SMS OTP and others) to a bare minimum. In the event of a high-risk score, a real-time alert is triggered for blocking the transaction. Low risk scores indicate on a strongly authenticated user (MFA) and a transaction which can be safely approved.

About Paygilant

Paygilant is a revolutionary frictionless digital banking and payments anti-fraud company. It is designed to eliminate the trade-off between strong fraud prevention, frictionless authentication, and user privacy.

Paygilant enables financial organizations to boost their revenue, by enhancing the user experience and preventing fraud before the transaction occurs. It's easy-to-integrate patented technology, utilizes six proprietary Intelligence Sets, which work in harmony to deliver value from day-one. Paygilant simply triggers a real-time "risky" indication when fraud is detected, and a "safe" indication when the legitimate customer has been authenticated.

Paygilant office: 10 Ben Gurion Road, Ramat Gan, Israel
E-mail: info@paygilant.com | Phone: +972-3-5221879