Fraudless. Frictionless. Effortless.

The Importance of Mobile Being First

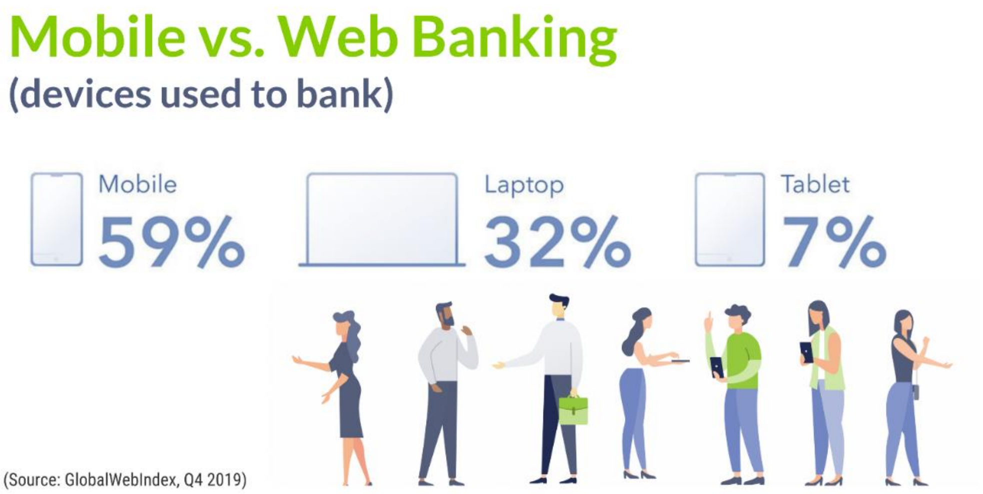
Mobile vs. Web Fraud Prevention

During the past year coronavirus lockdowns and social distancing have completely transformed the payments landscape. Face-to-face transactions have been replaced by new and emerging digital payment methods, and fraudsters are exploiting the accelerated shift to digital payments.

According to a recent study by Javelin Strategy Research and SAS, digital fraud keeps being a global, multibillion-dollar phenomenon. While digital payments are fast, fraud moves just as fast.

Digital fraud can be divided into two main sectors: web fraud and mobile fraud. While both channels come with significant fraud losses, current fraud prevention techniques are not sufficient to equally reduce fraud in both channels.

While the methods fraudsters use are evolving, organizations have deployed multiple anti-fraud controls, to keep web-based fraud at bay. According to a report by CyberSource, the fraud rate for online transactions (not including mobile) has been steady since 2010. As the motivation of fraudsters to cash-out has not decreased, the conclusion is that fraud shifts to the fast growing, less protected mobile channel.



(Source: GlobalWebIndex, Q4 2019)

Mobile fraud has increased by 170% during the last two years and the use of mobile banking and payments during the pandemic has also exasperated matters. In June 2020, the FBI reported that with the 50% surge in mobile banking since the beginning of the year, the risk of fraud is increasing, respectively. App-based banking trojans and fake banking applications were among the variety of techniques the FBI said it expects fraudsters to employ.

In 2020 Fraudsters continued to migrate away from web based fraud with 62% of attempted payment fraud attacks coming from mobile devices – up from 51% in 2019.

In 2020 fraudsters migrated away from web-based fraud with 62% of attempted payment fraud attacks coming from mobile devices up from 51% in 2019.

(Source: Yahoo Finance, 2021)

Online Fraud Security

Online fraud has been an issue since the beginning of e-Commerce in the early 90’s. The internet was a new concept and businesses were not totally aware of its risks. The first online scams came in the form of fraudsters using stolen credit cards and ascribing them to popular celebrities of the time. Mass online identity theft followed. These events sparked the birth of online fraud security and a slew of innovations suitable for web:

Anti-malware Programs

These are implemented on the server and endpoint to guard against malware acquired online that can be used to steal a person’s identity or credit card information.

Site Encryption

This is implemented by the website owner to protect users browsing the web. This is especially useful when using un-secured, public Wi-Fi connections.

Geolocation

This is implemented on the business-end and identifies the location of a device to detect fraud. Location of a desktop can be determined using WIFI or IP geolocation.

Mobile Fraud Security

Mobile fraud refers to the attempted or successful fraudulent transactions carried out in a mobile environment, either via a mobile application or the browser of a mobile device. Mobile fraud sometimes takes advantage of weaknesses inherent to applications that are tied to Challenger/Neo banks, eWallets and mCommerce. Gaining access to a mobile device banking app or the eWallet, opens up easy opportunities for fraudsters to exploit. Examples of mobile fraud include fraudulent P2P, mCommerce transactions, fraudulent buyer/seller collusion within a mobile marketplace, and payment accounts taken over and funds defrauded using a smartphone.

Mobile fraud can also be perpetrated by fraudsters who do not actually use a mobile device. This is done using 'emulators' which enable the criminal to appear, as if they're connected from a mobile device. Such tools enable them to make purchases via mobile apps or mobile websites, while in fact a laptop or desktop computer is being used. This provides the fraudsters enormous scalability and flexibility by pretending to come from a different location and appearing to be using a different device for every transaction / victim.

Web vs. Mobile

Many of the methods commonly used to secure web transactions are not effective for mobile devices. For example, mobile IP addresses are constantly changing as a user roams among networks. Users also upgrade their phones occasionally to stay up to date with the newest models. These make it difficult to gain any solid information and detect fraud. The fact that mobile devices are by nature "mobile" presents a challenge for proponents of traditional fraud security.

While behavioral attributes can be captured on browsers, such data is not as diverse. Browsers are limited to mouse and key-board dynamics. In a world where data is everything, a lesser amount of data means a weaker behavioral profile. Moreover, web based behavioral biometrics solutions, tend to generate more false positives. This is another reason the mobile channel presents a unique opportunity for organizations to upgrade their fraud prevention guards, by using new methods that decrease friction, false positives, and increase security.

In the mobile fraud world, the diversity and quantity of fraud indicators, have become the leading methods of fraud prevention:

Device Fingerprinting

This is implemented to identify a specific device based on its unique characteristics. This is one of the most common and effective methods used for detecting fraud and verifying returning users.

Behavioral Biometrics

Behavioral biometrics is used to detect non-human activity and authenticate customers. Mobile touchscreens are equipped to gather large amounts of data like fingerprint size, pressure, swiping behavior, and more. Mobile devices have the potential to gather heartbeat data and vein patterns. A touchscreen can discern whether a user's palms are sweating or not. Businesses continue to innovate and discover new ways for mobile devices to gather behavioral data. Thus, data attributes used to indicate whether an individual is legitimate or a fraudster are more often correct.

Transaction Analysis

Transaction analysis is mainly based on client profiling and transaction habits. It analyzes transaction data (amounts, beneficiaries, frequency, etc.) but also metadata associated to each operation (for example - location of a transaction payment, smartphone location).

Such data gathered opens a new dimension for the analysis of clients' identity. Unlike traditional KYC, representing a rather static picture of the client, a 'digital identity' can dynamically assess client behavior by analyzing transaction data (amount, beneficiary, issuer) and its associated metadata. The level of client knowledge and security is then enhanced through the combination 'who the client is' and 'what the client does.'

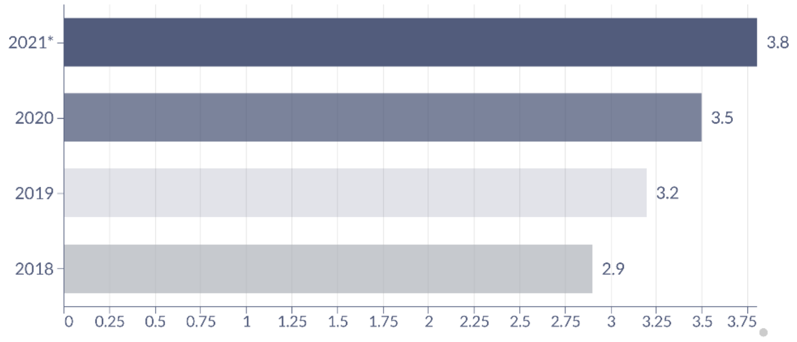
The Future of Fraud Prevention

It is important to recognize that web and mobile channels are different. What works for desktops will not automatically work for mobile devices.

The reality is that Gen Z, Millennials and in fact all of us increase the use of our mobile devices, while decreasing the usage of a computer. That said, companies need to get with the times or be left behind. This entails adopting more advanced and effective fraud prevention methods to ensure a great user experience, while avoiding money loss.

Worldwide by 2021, there will be 3.8 billion smartphone users, and it has been predicted that the count of the same will gradually increase year by year.

Worldwide Use of Mobile Devices (2018 -2021)



Mobile-First Growth (And Risk)

It's a fact that fraudsters follow the money, and with the steep growth in global transactions taking place via mobile phones, it is a profitable hunting ground for fraudsters. That is why it is imperative that businesses and financial institutions take a closer look at their mobile fraud prevention strategies and controls. Many financial institutions use outdated risk management systems built on manual processes — a remnant from the days when customers visited their financial institutions in person to apply for loans, withdraw money and carry out other banking activities. The very nature of mobile apps requires a change in banks' risk management systems.

eCommerce sites too are also trying to adapt existing solutions to mobile when it is a far better mindset to think about fraud prevention solutions specifically designed for the mobile channel. As there is no silver bullet to eradicate mobile fraud, organizations must consider mobile-first fraud prevention methods as a primary lifeline.

In the digital world, a person's device acts as their online identity. It is also one piece of "identity" that is much tougher for fraudsters to continue replacing, as opposed to easily swapped out online identifiers like email addresses. Distinguishing customers' devices through their unique characteristics and analyzing them independently of personal data, allows businesses to verify transacting devices and verify the connected customer. When it comes to mobile banking, strong customer authentication (SCA) may even eliminate the need for secondary authentication steps for positively identified trusted devices which greatly reduces customer friction.

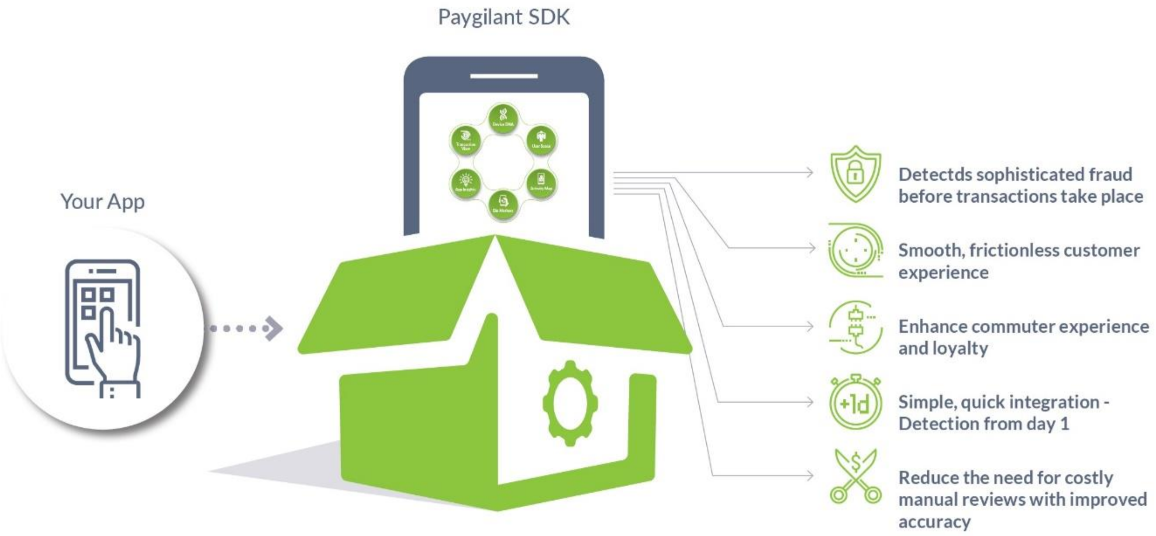
An additional option banks and businesses can turn to in the fight against mobile fraud, is a mobile SDK (software development kit) solution. Fraud prevention Mobile SDKs can be easily integrated into the existing app, with a short code snippet that allows businesses to detect high-risk anomalies across all mobile payment and banking platforms (eWallets, mobile banking apps, one-click payments, etc.). The help of machine learning in such solutions can detect tampered devices, the presence of a stolen identity and even the increasingly ubiquitous new account & synthetic fraud and account takeover fraud. This allows for instant and confident acceptance of on-demand activity within a native mobile application, whether it be a large bank withdrawal or an expensive eCommerce purchase.

For many vendors mobile transactions can be more secure than web transactions; while for users, mobile authentication can provide low friction authentication. The basic principle is that individual devices can be securely identified, while individual users can be tied to the device via multiple fraud indictors. A layered approach that includes a combination of device fingerprinting, behavioral biometrics, machine learning, and transaction analysis can help you detect mobile fraud, maximize your approval rates as well as contain your new application and transaction fraud.

Paygilant – A Mobile First Solution

Paygilant's solution is designed as a mobile-first solution. What makes Paygilant unique is that 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 mobile 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.


Paygilant SDK
Your App
Device DNA
User Score
Activity Map
App Insights
Detectds sophisticated fraud before transactions take place
Smooth, frictionless customer experience
Enhance commuter experience and loyalty
+1d
Simple, quick integration - Detection from day 1
$
Reduce the need for costly manual reviews with improved accuracy

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 and eCommerce organizations to boost their revenue, by enhancing the user experience and preventing fraud before the transaction occurs. Its 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” score when fraud is detected, and a “safe” one when the legitimate customer has been authenticated.

paygilant

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

paygilant.com