



# ThreatMark

ThreatMark

## Mobile Banking Fraud

Secure Your Mobile Channels, Using State/of/Art Solution from ThreatMark

Today, most of the payment transactions are performed via mobile devices. Mobile technology has made the security challenges much more complex as fraudsters are becoming more sophisticated and try ever changing attack vectors through mobile specific and cross-channel attacks.

Our solution is engineered in a unique way to provide multilayer security for mobile channels by combining **Deep Behavioral Profiling** with powerful **Threat Detection Engine**.

### Threat Detection:



By integrating with any native mobile application our lightweight mobile Anti-Fraud component will protect clients against mobile threats such as overlay attacks, mTAN interceptions, keyloggers, SMS grabbers, banking trojans, mobile-based identity theft attacks and cross-channel attacks.



Security checks to detect rooted/jailbroken devices, insecure networks being used, or malicious applications and tools being installed will help your organization to monitor all your applications running in non-trusted environments. Using user configurable policies and risk assessment such devices can be reported in real-time and transactions performed from such devices can be put on a watch list.

@ThreatMark

linkedin.com/company/ThreatMark

Contact us at [sales@threatmark.com](mailto:sales@threatmark.com)

[www.threatmark.com](http://www.threatmark.com)



Fraudsters are also trying to take advantage of decompiling application and using reverse engineering to engage communication between mobile and server. Our solution detects application tampering scripted attacks and hacking attempts effectively ensuring your application is self-protected and its security is not jeopardized.







If any application contains malicious, suspicious code or has potentially dangerous permissions, it will be flagged in real time. Unknown threats are sent for further review to our SOC (Security Operation Center) allowing you to rapidly respond to even 0 - days attacks.

## User Identity Verification:



Behavior of each user interacting with the mobile device and the mobile application is continuously monitored by the system and compared using machine learning methods with previously learned behavior. In case that the current user's typing speed, swipe gestures, navigation patterns and other behavioral traits are strongly different to the legitimate user an alert is raised at the backend showing that there is an ongoing account takeover attempt. Each device is also fingerprinted and compared with our anonymized global database of fraudulent and legitimate devices.

Big Data Analytics				Layer 5
Device aware	Session aware	User aware	Transaction aware	
Layer 1	Layer 2	Layer 3	Layer 4	
<p><b>Access</b></p> <ul style="list-style-type: none"> <li>• Connection check (TOR, anon proxy)</li> <li>• Browser and OS security check</li> <li>• Malware, phishing</li> <li>• Device fingerprint</li> </ul> 	<p><b>Logon</b></p> <ul style="list-style-type: none"> <li>• GeolP check</li> <li>• Login time check</li> <li>• Logon biometrics</li> <li>• Velocity checks</li> <li>• Action context</li> </ul> 	<p><b>Navigation</b></p> <ul style="list-style-type: none"> <li>• Clickstream profiling</li> <li>• Scripted access and automation detection</li> <li>• Session hijacking</li> <li>• Behavior and app interaction biometrics</li> </ul> 	<p><b>Transactions</b></p> <ul style="list-style-type: none"> <li>• Money mule blacklist</li> <li>• Anomalous transactions</li> <li>• Behavioral profiling</li> </ul> 	



@ThreatMark

linkedin.com/company/ThreatMark

Contact us at sales@threatmark.com

www.threatmark.com