ThreatMetrix®
BUILDING TRUST ON THE INTERNET™

WHITEPAPER

# Fraud Protection for Native Mobile Applications

## Benefits for Business Owners and End Users

## Table of Contents

The use of smart phones, tablets, and other mobile devices to conduct online transactions has rapidly grown into a standard practice. Crime associated with these mobile devices has increased proportionally, and businesses have a critical need to detect and prevent fraud related to them.

This white paper describes how ThreatMetrix™ helps businesses prevent the commission of fraud via mobile devices. To be more precise, it covers the use of native mobile apps, and how businesses can a) detect and prevent fraud when they are used, and b) make transactions from mobile apps more simple and secure for end users.

When transactions are enacted via traditional desktop browsers, or standard default browsers on mobile devices, ThreatMetrix fraud prevention systems are able to perform advanced profiling of the device, uniquely identify it, and establish a trust score that identifies the level of fraud risk.

However, native mobile apps downloaded to a phone or tablet are designed for a specific website or web application, and are lightweight in comparison to traditional browsers. They don't generally have the infrastructure required to positively identify the device and adequately determine risks or threats it may present. Unless the mobile app is upgraded and equipped with the necessary infrastructure and intelligence, trust cannot be properly established, and the user may experience rejection or step-up authentication. Unfortunately, adding the necessary technology and controls requires a great deal of work and very specific knowledge, both of which are generally outside the experience of most mobile application developers.

To address these problems, ThreatMetrix provides a lightweight library, in the form of a software development kit or SDK, that developers can easily integrate within their mobile apps. This SDK, known as TrustDefender™ Mobile, provides mobile apps with the infrastructure and intelligence needed to verify the trustworthiness of the mobile device. Legitimate users of such apps are immediately recognized as such, and can conduct their transactions without having to respond to additional authentication procedures in order to verify their identity. In this manner, TrustDefender Mobile provides benefits for both business owners and their customers or end users.

TrustDefender Mobile is a fully-integrated component of the TrustDefender Cybercrime Protection Platform, which provides full context-based authentication and fraud prevention for websites and web applications. As a fully-integrated component, TrustDefender Mobile enjoys all of the full platform's features, benefits, and advantages.

A discussion of the complete TrustDefender Cybercrime Protection Platform is outside the scope of this paper, and readers are encouraged to consult other ThreatMetrix documents to learn more about the platform as a whole. For our purposes here, the important thing to remember is that TrustDefender Mobile is part of, and uses, the full platform's infrastructure.

## How TrustDefender Mobile Works

Organizations use ThreatMetrix to detect and prevent fraud by invoking TrustDefender Mobile to protect key interactions—typically during login, payment, and account registrations. When users perform these actions, the TrustDefender Mobile code embedded within the app provides an advanced and detailed threat and risk assessment of the mobile device. The device is uniquely identified and analyzed for the presence of malware. Additionally, numerous attributes are gathered to indicate whether the device is configured normally, or has suspicious settings or other anomalies indicating risk.

TrustDefender's unique mobile device analysis profiles devices for the following information:

- **Persistent Device Identification:** This feature identifies individual mobile devices for both iOS and Android platforms, even if the device has been reset or the application has been reinstalled.
- **Location Services:** Gathers latitude and longitude information from the GPS hardware, and compares IP addresses with physical locations to detect the use of proxies and VPNs. Rated to be accurate within meters, and can be configured to prolong battery life.
- **Detects Jailbreak (iOS) and Rooted (Android) Devices:** Dynamic jailbreak and root detection technologies determine when device security controls have been thwarted. New jailbreak and root methods are pulled from the TrustDefender server each time a device is profiled, to keep the system up-to-date without requiring new application releases. This feature can report the actual number and method names of the jailbreak and root technologies being used.
- **Malware Detection:** For Android-based systems, TrustDefender Mobile verifies the integrity of the application in which it is embedded to ensure it has not been compromised or infected. It also analyzes all other apps installed on the device and reports their reputation and the presence of tampering or malicious code.
- **Anomaly Detection**—This feature detects device tampering as well as attempts to masquerade as a different device, along with a number of other anomalies that may indicate fraud.
- **Packet Fingerprinting** – Automatically detects device and data spoofing via analysis of the network traffic packet signatures originating from the device.

TrustDefender Mobile also includes five custom-defined attribute fields, allowing application designers to create their own attributes and have them evaluated by the policy engine.

## Unique Capabilities and Technologies

TrustDefender Mobile contains a number of capabilities and advanced technologies unavailable in other solutions. TrustDefender Mobile is effective at detecting whether a device has been compromised or disguised, or if its use is likely to be risky or associated with fraudulent activity.

### Host Application Integrity Check

For Android-based systems, TrustDefender Mobile performs an integrity check of the application in which it is embedded (i.e. the organization's mobile app), verifying that the application is a genuine and unmodified version. For example, if a bank uses TrustDefender Mobile to protect its online banking application, any infection or unauthorized change would be detected.

### Malware Detection

For Android-based systems, TrustDefender Mobile analyzes and verifies the integrity of all apps installed on the device. When a user connects to a ThreatMetrix protected web application, signatures of all apps on the device are passed to the TrustDefender Cybercrime Protection Platform. The platform first verifies the integrity of the organization's mobile app, then, using a data feed from Webroot's Cloud Mobile App Reputation Service, verifies all apps present and reports on their reputation. Clean apps are identified and any apps that are compromised, contain malware, or have poor reputations are detected and reported in real-time.

ThreatMetrix employs a number of methods to ensure that the malware detection features of TrustDefender Mobile don't degrade mobile device performance. For example, signatures of each app are stored locally on the device itself. This makes the data instantly available – averting the need to re-scan each time the user connects. Similarly, all mobile app reputation and other relevant data from Webroot is stored on the TrustDefender Cybercrime Protection Platform. Calls to Webroot only occur when a new mobile app is discovered and its data does not yet exist in the ThreatMetrix Platform. These capabilities make TrustDefender Mobile's malware detection extremely efficient and effective.

### Dynamic Configuration and Updates

TrustDefender Mobile is uniquely designed to minimize application updates. Because it can be dynamically updated and configured by ThreatMetrix's cloud-based servers, it is not necessary for organizations to re-release the app, or force updates to change configurations or receive the latest threat intelligence. For example, malicious users are constantly developing new methods, such as jail-breaking or rooting, to disable a device's security features. Dynamic configuration and updating give TrustDefender Mobile access to new threat data without requiring the app itself to be updated.

## Advanced and Persistent Device Identification

Identifying mobile devices has always been a challenge for application developers. Fraudsters deliberately remove built-in security controls and modify device identifiers. A device may be reset, altering its attributes, or the identifying app itself may be reinstalled. Device identification codes must also be compliant with app store publishing and privacy guidelines. All of these factors make accurate device identification difficult to achieve.

Fortunately, ThreatMetrix has extensive experience identifying mobile devices, and has spent years developing advanced technologies capable of accurately identifying each and every specific device. TrustDefender Mobile can identify individual smart phones, tablets, or other devices, even when fraudsters intentionally alter device identities.

## Shared Global Trust Intelligence Network

TrustDefender Mobile is a fully-integrated component of the TrustDefender Cybercrime Protection Platform and benefits from being part of the world's largest and most comprehensive fraud intelligence network.

ThreatMetrix Shared Global Trust Intelligence Network profiles tens of millions of users and their devices daily, and regularly processes hundreds of millions of logins, payments and account creations. The data stored in the Global Trust Intelligence Network is used to evaluate users and their behavior, as well as their associated devices from all channels—including desktops, laptops, web browsers, and mobile devices running browsers or native apps.

Risk scores are derived from global network data, transaction data, as well as from sophisticated device profile information provided by ThreatMetrix components.

## Persona DB

Persona DB is an extensible, enterprise-accessible database that allows an organization to privately and securely store and retrieve identifying attributes, characteristics, and behaviors associated with its users and customers. Information relevant to customers or employees can be stored in the database. This can include data such as the exact mobile and other devices customers use, their access habits, normal locations, IDs, accounts, shipping addresses, and data necessary for step-up authentication such as mobile phone numbers or email addresses. The database may also contain IP or email addresses that have been compromised, previous associations with cybercrime or fraud, compliance data such as OFAC-banned countries, and countless other data elements.

Data stored by organizations within the Persona DB, along with information available from ThreatMetrix device profiling and the shared Global Trust Intelligence Network, is used to establish a unique Persona ID for each user or customer. This comprehensive data set allows ThreatMetrix to perform detailed user, device, and behavior analytics for every access and transaction in real-time, resulting in an unprecedented level of actionable intelligence and visitor risk-scoring capabilities. Armed with this information, businesses can create application policies to allow/deny access or approve/disapprove transactions with higher levels of accuracy and confidence.

## Trust Tags

Trust Tags provide sophisticated and powerful intelligence to help organizations detect hackers and fraudsters, speeding up the process of trusting legitimate employees and customers.

Trust Tags are digital labels stored within the Global Trust Intelligence Network. They can be applied to any entity in the network, including, but not limited to, users, devices, email addresses, login IDs, or any combination thereof, including mobile devices with native apps. This unique technology can be used to instantly identify trusted or untrusted situations that can't otherwise be determined. Trust tags can positively associate users, their devices, and their account logins to ensure a frictionless experience when all three entities are seen together. For example, Trust Tags can be used to grant instant access to specific users of a mobile app, even if their locations are blacklisted. Trust Tags have many other benefits, and readers are encouraged to refer to other ThreatMetrix documentation that describes their use and benefits in full.

## Part of a Large Family of Related Solutions

Many fraud prevention solutions require multiple modules or products to constitute a complete solution. TrustDefender Mobile, on the other hand, is completely integrated within the TrustDefender Cybercrime Protection Platform, which provides comprehensive fraud protection and context-based authentication.

## Easy Integration

TrustDefender Mobile is easy to embed within mobile applications. Mobile app developers simply include the TrustDefender Mobile library and, with a few lines of code, place calls to it in strategic situations, such as when a connection is made.

Integration can often be completed in a day or less. Since TrustDefender Mobile is completely compatible with existing tags, policies, and rules, no changes need to be made in the configuration or administration of the TrustDefender Cybercrime Protection Platform.

If desired, additional policies or rules can be added that are specific to a mobile app user base, such as a detailed analysis of GPS location data, or jailbreak/root detection and evaluation.

## Benefits for Businesses Organizations and Mobile App Users

### Increased Security and Reduction in Fraud-Driven Losses

Mobile app security is among the highest concerns of IT security, fraud specialists and end-user customers. Mobile apps frequently lack basic security features like two-factor authentication, HTTPS certificate validation, and complete end-to-end encryption between the device and the server. To make matters worse, fraud prevention systems have a difficult time profiling a device when a mobile app is used as the connection mechanism. Mobile apps generally lack the infrastructure required for fraud prevention systems to perform deep inspection of the device. For example, it's generally not possible to determine if a smart phone or tablet is masquerading as a different device, or if it has been compromised by malware. Even uniquely identifying a device can be difficult, rendering it challenging to associate specific devices with their users.

TrustDefender Mobile deploys the most advanced technologies to profile devices running native mobile apps. This profiling dramatically increases security, and empowers organizations to detect high-risk transactions, thereby significantly reducing fraud-related losses.

### Increased Revenue

The number of mobile apps continues to skyrocket, and with good reason. They make it easier for users to navigate and interact with websites and applications. Businesses also benefit in many ways, including increased mobile orders, push notifications, loyalty rewards, and social referrals, to name a few. Numerous studies have shown that revenues increase when mobile apps are made available to customers and consumers.

The increased security provided by TrustDefender Mobile can give organizations the confidence and tools they need to fully utilize mobile apps. And because good customers can be instantly identified, fewer are rejected, leading to an increase in revenue.

### Easier and More Secure Access For Mobile App Users

End users will appreciate knowing that the app they are using has sophisticated security features to help protect them from identity theft, account takeover, and other types of fraud.

Additionally, because TrustDefender Mobile enables transparent, frictionless two-factor authentication, end users are not burdened with extra authentication procedures. This will make their overall experience with the app and associated websites much more pleasant.

### Low TOC

Implementing TrustDefender Mobile is a fast and cost-effective way to protect the integrity of web applications and online transactions. Because the corresponding TrustDefender Cybercrime Protection Platform is a cloud-based solution, it requires no installation, and there's no hardware or software to manage.

Most organizations that deploy TrustDefender Mobile experience a full return on their investment within months.

## Summary

The security concerns raised by the recent explosion in the use of mobile apps' are likely to stay with us for a long time. Many organizations stand to benefit by providing these highly-effective applications to their customers and consumers.

Many mobile apps, however, are alarmingly deficient when it comes to security and fraud protection. Fortunately, it's easy for developers to embed TrustDefender Mobile within their apps— and protect themselves and their customers with the most advanced fraud protection available.

## About ThreatMetrix

ThreatMetrix builds trust on the Internet by offering market-leading advanced fraud prevention and frictionless context-based security solutions. These solutions authenticate consumer and workforce access to mission critical applications using real-time identity and access analytics that leverage the world's largest trusted identity network.

ThreatMetrix secures enterprise applications against account takeover, payment fraud, fraudulent account registrations, malware, and data breaches. Underpinning the solution is the ThreatMetrix® Global Trust Intelligence Network, which analyzes over 850 million monthly transactions and protects more than 210 million active user accounts across 3,000 customers and 15,000 websites. The ThreatMetrix solution is deployed across a variety of industries, including financial services, enterprise, e-commerce, payments, social networks, government and insurance.

## For More Information:

For more information about the TrustDefender Cybercrime Protection Platform, including TrustDefender Mobile, visit our website at **www.threatmetrix.com.**

**ThreatMetrix Inc.**
160 W Santa Clara St. Suite 1400
San Jose, CA, 95113
Telephone: +1 408 200 5755