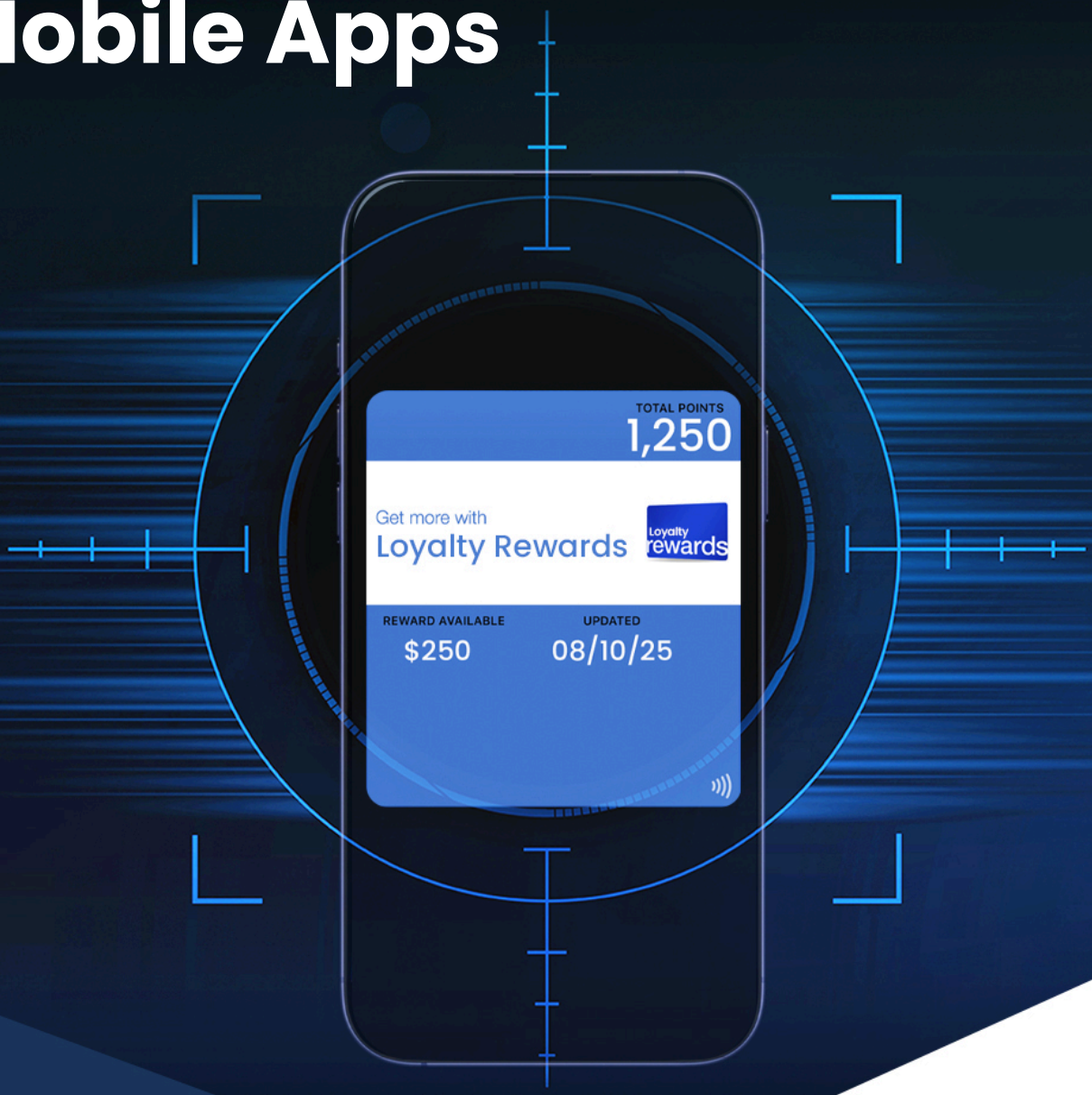
Zimperium Prevents Loyalty Fraud in Mobile Apps



MAPS™

ZIMPERIUM®

Loyalty and rewards programs have evolved well beyond simple points and discounts. Today, users can:

- Pay directly with points at checkout
- Convert points to cash or prepaid value
- Exchange points across ecosystems and brands
- Store and redeem rewards via digital wallets like Apple Wallet or Google Wallet

These capabilities are powered by integrations with third-party rewards platforms that merchants pay for—either through flat licensing fees or a percentage of each redemption. This means there is a **direct cost to the business** every time a reward is redeemed—fraudulent or not.

How Mobile Apps Are Used to Abuse Rewards

Most rewards today are redeemed via mobile apps, making them the central access point for attackers. In fact, studies show that over **60% of loyalty program members prefer using mobile apps** to access and redeem rewards. This preference, combined with the ease of integration into digital wallets and rewards marketplaces, makes the mobile app the most exposed and abused surface for loyalty fraud.

Here are the most common types of fraud and abuse enabled via the mobile app:

1. **Fraudulent Redemptions**
   Attackers gain unauthorized access to real customer accounts via malware to steal loyalty assets (points, gift cards, discounts) or make fraudulent redemptions.

2. **Fake Accounts Abusing Offers**
   Fraudsters utilize bots, scripts, and device farms to create thousands of fake users and accounts that exploit welcome bonuses, referrals, and other loyalty incentives.

3. **Promotion Abuse**
   Attackers inspect and abuse the mobile app to bypass controls and repeatedly trigger coupons, referral codes, or reward events.

How Mobile App Protection Secures Loyalty Programs:

Zimperium's Mobile App Protection Suite (MAPS) stops loyalty fraud where it starts—on the mobile device and inside the app. Unlike traditional server-side API security solutions, mobile app protection provides deep, on-device defenses that prevent abuse before it hits backend infrastructure.

Here are the key MAPS capabilites that prevent loyalty fraud:

App Hardening

- Makes reverse engineering the mobile app significantly harder
- Obfuscates API endpoints, keys, and redemption logic
- Prevents app tampering and code injection
- Prevent repackaging apps with malware
- Prevent the app from running on an attacker's devices

Runtime Protection

- Prevent the app from running on devices that are prone to abuse, such as jailbroken/rooted devices, and emulators.
- Blocks and limits app execution on compromised devices or unsafe Wifis.
- Prevents malware from stealing credentials via overlays, accessibility abuse, and similar techniques
- Enables the app to verify the device's integrity before running at all times.

Threat Analytics

- Gain insights into patterns like fake sign-ups, referral abuse, and unauthorized redemptions via the app before they scale.
- Get real-time security alerts on cloning, tampering, and account takeover attempts.
- Correlate app security signals (e.g., jailbroken devices, fake devices) to loyalty program abuse and revenue impact to prioritize responses.

Zimperium is already helping leading airlines and retail gas station businesses protect their loyalty and rewards programs from mobile app abuse. By securing the app itself, these organizations prevent fraud, preserve customer trust, and safeguard revenue.

Ready to Secure Your Loyalty Program?

Let's talk about how we can help you stop fraud at the source—inside your mobile app.

Contact Us or reach out to your Zimperium representative to learn more.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244