AperioGuard Issues Industry Alert: 2026 Trial Abuse Projected to Spike 4X as "First-Party" Fraud Costs Reach $100B

AperioGuard identifies critical gaps in modern identity matching and payment logic, providing engineering teams with tactical blueprints to weld shut revenue leaks.

New York City, New York May 14, 2026 (Issuewire.com) - Security forensics firm **AperioGuard** is alerting to the new wave of "first party fraud," as trial abuse loses skyrocket to an estimated **$100 billion** annually by **late 2026**. Using a "Zero-Footprint" audit program and a manual stress test approach to discover revenue drains with no risk of data compromise, the company is transitioning away from a defense against "burner emails" to a guard against sophisticated session-interception and constant identity-masking schemes that automated systems were not engineered for.

As AI-as-a-Service (AIaaS) has become ubiquitous, advanced threat actors are exploiting "Adversary-in-the-Middle" (AiTM) kits to overcome Multi-Factor Authentication (MFA) and payment gate technologies. "First-party" fraud, also known as exploiting free resources through constant sign-up/abandonment of multiple identities, is now invisible to rules-based systems as **68%** of fraud decision-makers admit they are not adequately prepared to address these risks.

In response, AperioGuard is releasing a new version of its "Zero-Footprint" Forensic Protocol, a manual stress-testing approach that targets trial logic in a manner analogous to how malicious attackers exploit products without accessing codebase or admin credentials.

"Traditional fraud prevention solutions are antiquated; abusers are leveraging AI for industrialized, scaled exploitation," said the **Founder of AperioGuard, Michal Rauch**. "Gone are the days of just

simple burner emails, replaced by session-interception and identity-persistence tactics that existing systems were not built to stop. Our goal is to equip engineering teams with a forensic Guidebook that addresses the root cause, not the symptoms."

A Zero-Access Approach to Security Auditing

The AperioGuard protocol provides engineers with concrete information regarding the vulnerabilities that lie at the intersection of identity matching and payment logic and those that account for a significant portion of the **$100 billion** annual losses from first-party fraud. With an attacker's-eye perspective, AperioGuard's manual analysis ensures that hard-coded solutions can address the revenue leaks before they impact unit economics.

About AperioGuard

AperioGuard specializes in forensic trial abuse prevention across the globe. Leveraging "Zero-Footprint" forensic analysis, the firm provides external, manual stress testing that pinpoints critical revenue leakages, removing the risks of integrated system analysis.

Media Contact:
Michal Rauch,
Founder & Director of AperioGuard
michal@aperioguard.com
www.aperioguard.com

Media Contact

AperioGuard

*********@aperioguard.com

https://aperioguard.com

Source : AperioGuard

See on IssueWire