HID Risk Management Solution

Introducing the HID Risk Management Solution (RMS) — a comprehensive approach to safeguarding all digital banking channels and empowering organizations to effectively identify, assess, mitigate and monitor risks. This powerful solution offers a holistic defence against fraud, ensuring a secure and trustworthy digital experience for banks and financial institutions. With HID's Risk Management Solution in place, organizations gain the tools and capabilities to build a seamless and reliable digital experience for their users. By implementing this cutting-edge solution, they can stay one step ahead of potential online threats and fraudsters all by creating a safe environment and protecting their channels, user identities and their valuable assets.

HID RMS offers a unique, layered defense approach, which ensures comprehensive, multilayer protection against digital fraud. Its fast implementation, zero impact on customer infrastructure, and cost-effectiveness make it an ideal solution for businesses seeking to bolster their fraud management strategies without disrupting their existing operations.

KEY BENEFITS

- **Comprehensive Fraud Detection:** RMS is built on a unique, multilayered defense approach that focuses on early warning and detection capabilities, knowing your customers and transaction risk analysis in combination with HID's robust portfolio of consumer authentication solutions. It detects a wide range of fraud types, including account takeover, new account fraud, phishing, SIM swap, vishing, bot attacks, malware, RAT attacks and more.
- **Compatibility:** Works on all devices across all channels through one integrated analytical engine
- **Customization:** Fully customizable to fit your business needs and policies with a graphical editor and robust rule engine
- **Modular Architecture:** Can be used as a primary anti-fraud solution or as an addition to existing fraud management, effectively filling gaps in fraud and cyber threat protection layers
- **Real-World Use Case Solutions:** RMS effectively addresses real-world fraud scenarios, providing practical solutions to account takeover, authorized push payments scams, bot attacks and more
- **Risk-Based Authentication:** Provides strong customer authentication (SCA) when paired with HID Authentication Service, offering best-in-class, risk-based authentication
- **Fast Implementation:** Quick proof of concept with real-time responses, ensuring rapid time to value
- **Zero Impact:** No impact on customer infrastructure; can augment existing fraud solutions deployed by the customer
- **Cost-Effectiveness:** Enriches data consumed by other fraud tools, reducing friction and costs

HID Risk Management Solution

KEY USE CASES:

- **Account Takeover:** RMS can detect suspicious activity related to account takeover attempts. It utilizes device location, biometrics and continuous user profiling to adapt to changes in data, allowing for an adaptive response to potential threats.
- **Authorized Push Payment Scams:** RMS can identify suspicious activity and behavior related to authorized push payment scams. It monitors factors such as active call sessions, session lengths and unusual customer behavior (e.g., new beneficiary, unusual amounts, etc.).
- **Anti-Bot Measures:** RMS can differentiate between human and bot actions, stopping automated and brute force attacks. It can also detect the use of remote access tools.
- **Social Engineering Scams:** Fraudsters exploit fear, emotions and ignorance to manipulate and target unsuspecting individuals as easy prey. RMS leverages a combination of data points such as session length, active call, accelerometer, gyroscope, geolocation, etc., to determine a risk score and accurately tag social engineering attacks. As a result, banks can dynamically tailor their intervention strategies to effectively counter these threats.
- **Mobile Banking Threats:** Between 75% to 90% of the digital banking journey happens via mobile phones. RMS safeguards mobile channels and devices against potential targeting and breaches. It identifies indicators like jailbroken devices, malware presence, remote access attempts, app misusage, emulator detection and numerous other factors in real time.
- **PSD2 Compliance:** HID RMS is designed with PSD2 requirements in mind, addressing transaction monitoring, transaction risk analysis and secure authentication of requests initiating from third-party providers.

	HID RMS
Available Platforms	JavaScript SDK for web browsers on any OS Native iOS and Android SDK
Enables Compliance	GDPR (Europe) CCPA (California/USA) PIPEDA (Canada) The customers are notified of the purpose of data collection and recipients of the data
Intelligence Factors and Checks	Device Awareness • Device reputation • Device fingerprint • Jailbreak/root check Application Awareness • Application debugging • Application cloning • Emulator detection Session Awareness • Known bad IP address • IP reputation checks • Geolocation • Geo-velocity/impossible journey User Awareness • Behavioral analytics • Known user on new device • Navigation behavior Transaction Awareness • Payment anomalies/behavior • Payment rules & alerts • Mule/fraudster accounts • Shared fraud schemes

hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here

2024-03-27-iams-risk-management-solution-ds-en PLT-05632
Part of ASSA ABLOY