KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

September 10, 2021

HID Global Fraud Prevention Offering

HID Global offers robust and secure solutions for identity and access management, including a highly scalable authentication platform, physical access controls, smart identity card manufacturing and credential issuance, biometric authentication, and fraud prevention in the form of mobile/remote identity proofing, real time threat detection and strong security protocols and cryptographic standards to secure digital channels. HID Global presents each of these elements into a full fraud prevention offering suitable for helping customers reduce the risk and costs associated with Account Take Over, New Account Fraud, and many other types of digital threats.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Fraud is a major cost to businesses worldwide. Multiple reporting sources estimate that total related cybercrime costs will reach \$10.5 trillion by 2025 globally. Banking, finance, payment services, and retail are some of the most frequent objectives of fraudsters, as expected. However, insurance, gaming, telecommunications, health care, cryptocurrency exchanges, travel and hospitality, and real estate are increasingly targeted as cybercriminals have realized that most online services trade in monetary equivalents. Moreover, after years in the sights of cybercriminals, banking and finance in general are better secured than other industries, so fraudsters attack any potentially lucrative target of opportunity. Fraud perpetrators also continually diversify their Tactics, Techniques, and Procedures (TTPs).

Three of the most prevalent types of fraud businesses experience today are:

Account Takeover Fraud (ATO) - Often occurs when fraudsters use breached passwords and credential stuffing attacks to execute unauthorized transactions. Additional means for account takeover fraud are malware attacks (man in the middle and man in the browser) as well as the use of Remote Access Tools via Trojan or social engineering scams.

New Account Fraud (NAF) -- Fraud that occurs at the time of account opening, also called Synthetic Fraud or Account Opening Fraud. This often happens as a result of using stolen personal information to create a synthetic digital ID, can be more difficult to detect and has advantages for attackers. This type involves gathering bits of PII (Personally Identifiable Information) on legitimate persons to construct illegitimate accounts. Educational, financial, and medical records can be sources of PII used for assembling fake accounts, which are then often used to abuse promotions and instant loans and/or used as mule accounts to move money around.

Social Engineering Voice Scams -- In this scam, also known as Authorized Push Payment fraud, fraudsters call up victims, pretending to be from a bank or other business, and ask them to perform fraudulent actions such as transferring funds immediately in response to a non-existent condition. Fraudsters may claim that the victim's accounts have been compromised and they need to move their funds as soon as possible to protect their money.

One of the chief mitigation strategies against these types of fraud is risk-based multi-factor authentication (MFA). Strong authentication or MFA can eliminate a substantial portion of ATOs by increasing authentication assurance levels. Risk-based MFA often utilizes mechanisms to increase identity assurance, such as identity proofing, user behavioral analytics, and behavioral/passive biometrics.

Risk-based MFA is characterized by transaction-time evaluation of multiple factors, including information about users, their devices, and the environments from which requests emanate. There are cases where legitimate users are being scammed (social engineering voice scams, for instance) and can pass the tests involved in various forms of MFA. The presence and action of malware like Remote Access Trojans (RATs)

may also taint the results of MFA risk analyses. Thus, it is important to be able to have deeper insights into the context of each transaction. Risk-based MFA solutions operate optimally when integrated with or informed by Fraud Reduction Intelligence Platforms (FRIPs). FRIPs provide to risk-based MFA and transaction processing systems the information needed to make more accurate decisions on whether or not transactions should execute. FRIP solutions generally provide up to six major functions:

- Identity proofing/vetting
- Credential intelligence
- Device intelligence
- User behavioral analysis
- Behavioral/passive biometrics
- Bot detection & management

To detect and mitigate ATO fraud techniques, FRIP solutions interoperate with transaction processing systems, evaluating the context of each transaction request against pre-determined policies (similarly to authentication decisions in risk-based authentication systems) and then outputting risk scores. In these use cases, customers of FRIP solutions usually must write a bit of code to have their transaction processing systems query the FRIP service providers' APIs. For example, a FRIP customer will collect transaction context information and transmit that as part of the API call to the FRIP service. The FRIP solution analyzes the transaction request context, gathers additional intelligence relevant to the user and request in real-time, scores it in accordance with customer-determined policies, then returns the risk score and potentially additional insights to the calling customer. The customer's transaction processing logic then executes, taking into consideration the risk score from the FRIP service.

FRIP solutions also help prevent New Account fraud. Various components can work in concert to deter fraudsters from being able to use fraudulently obtained personal information to create accounts. Identity proofing is a collection of processes that aim to ensure that the person attempting to create a digital account is the person they are purporting to be. These processes may include physical verification of presence with photo ID, or more modern means of using mobile apps to electronically match physical documents with the device operator. Credential and device intelligence can be used as part of the identity vetting process to deter synthetic fraud. Moreover, the development of user behavioral biometric profiles that can be set as baselines and analyzed at subsequent registrations can be a useful technique for stopping account opening fraud attempts.

Integration between advanced FRIP solutions and line-of-business applications in finance, insurance, and retail industries is a required technique to mitigate the ever-increasing frequency of and sophistication of fraudsters.

2 Product Descriptions

HID Global is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID Global's US headquarters is in Austin, TX. HID Global has developed their own range of IAM solutions and makes Physical Access Controls Systems, RFID tags and readers, biometric readers, smart cards, passports and some national identity cards, card readers, and mobile solutions capable of remote identity verification as well as push notification transaction signing. Their intersection of IAM, biometrics, and their SDK allows their platform to perform identity card issuance for several kinds of organizations. HID Global also offers incident response and site takedown services.

Together, the aforementioned capabilities form the basis of HID Global's fraud prevention capabilities. HID Global offers components including ID proofing, credential and device intelligence, behavioral biometrics, UBA, bot detection and secure transaction signing. The solution can be hosted on premise or as SaaS from EU and NA public cloud data centers. The SaaS version is ISO 27001 and SSAE 18 SOC 2 Type 2 accredited. The solution is based on a micro-services architecture, and can run in IaaS providers AWS, Azure, or Oracle cloud. Subscriptions are available Per-User Per-Year (PUPY). The solutions can also be installed at customer sites on CentOS, RHEL, or Windows.

2.1 Identity Verification Service

Fraud protection begins with identity vetting at the time of account creation. Government and highly regulated industries worldwide such as financial institutions utilize HID Global for authoritative attribute lookups, remote document verification, and electronic credential assignment. In the case of digital document proofing, users utilize the smartphone app to scan and register the authoritative documents, conduct a quick liveness test by taking a selfie, and perform real-time biometric matching. Digital identity verification can be used to increase identity assurance levels for self-registering consumers either on-location or remote.

Digital identity proofing has rapidly gained acceptance and has become a requirement to support fraud reduction for many consumer-facing businesses as a result of the pandemic. The SDK offers a low-code approach plus strong tamper resistance to allow customers to create their own mobile apps for consumer identities. The SDK also serves to enable EMV 3DS compliance for customer applications. HID Global's built-in identity proofing functions give it a distinct advantage over competitors that do not have these capabilities.

2.2 Risk Management Solution

The HID Global Risk Management Solution addresses many of the most prevalent fraud types: ATO, synthetic fraud, banking overlays and other malware designed to obtain user credentials, and SIM swapping. This solution can consider compromised credential intelligence from within their network of customers for runtime transaction risk scoring. External feeds of compromised credential intelligence are not available for analysis presently.

In order to perform User Behavioral Analysis (UBA), solutions must have access to historical data on user engagements. Data points commonly examined by UBA functions include user profile attributes and subsequent changes to the profiles; and login locations, times, dates, success/failure rates, and frequency. For financial transactions, questions such as "is the requested amount and intended recipient typical of what this user has successfully transacted before?" must be answered accurately and with the lowest possible latency. Thus, these risk decisions must evaluate past transaction details involving payees and amounts. HID Global allows customers to configure UBA data retention periods as needed.

HID Global's mobile SDK and JavaScript provides good device intelligence. These features can examine device type, advanced device fingerprinting, device history and reputation, jailbreak/root status, IP address, geo-location, and hundreds of other attributes. Application behavior is analyzed to prevent banking and other site overlay malware from tampering with sessions.

The mobile SDK enables the collection of behavioral biometrics, which measure how a user interacts with their keyboard, mouse, and mobile device. Historical behavior is baselined and updated for each user for runtime risk evaluations. Behavioral biometric data retention is designed to look at the last ten sessions per user, uniquely taking in to consideration that human behavior changes over time.. HID Global's implementation looks at a wide range of behavioral biometric attributes including keyboard/mouse interactions, swipe and touchscreen interaction analysis, gyroscopic analysis, and accelerometer analysis. Moreover, the mobile SDK can perform ambient light sensing and factor the results as additional parameters for environmental analysis. SIM swap attacks can be detected by evaluating the combination of device and behavioral biometrics telemetry.

Bots are often used to perpetrate credential stuffing attacks for the purpose of taking over accounts. HID Global's union of device intelligence, behavioral biometrics, and UBA enable basic bot detection. When bots are suspected the solution can then alert customers that a given session is suspected of being artificially generated, allowing the customer to determine what courses of action they may want to take.

HID Global's Risk Management System allows customers to prioritize risk factors. Customers construct policies using easy-to-follow flow chart representation within the policy authoring interface. This method of building risk policies is the current state-of-the-art within industry. The score output from the risk engine service to customers ranges from 0-1000 with four major action recommendations. The fraud analyst interface is very intuitive and includes a detailed timeline view to expedite investigations.

Customers engage the HID Global Risk Management System via REST APIs, which supports JWT, OAuth, OIDC, and SAML authentication. Out-of-the-box reports are available and additional access to internal analytics via API is on the roadmap. The service is secured using FIPS 140-2 cryptographic components

and supports role-based, attribute-based, and delegated access controls. Administrators authenticate using strong MFA methods such as FIDO and hardware tokens. The Risk Management System can output event information to Security Incident and Event Management (SIEM) systems. The solution however does not integrate with IT Service Management (ITSM).

HID Global Risk Management System is an intelligence source to their own Authentication Platform. In this case, it provides real-time risk decisions for the Authentication Platform, which can then force users to authenticate more strongly to lower the risk. Some customers deploy both, especially amongst organizations within the financial industry, to take advantage of the integrated fraud reduction and strong authentication capabilities. Support for Multi-Factor Authentication, transaction time risk analysis, and transaction signing enables financial customers to satisfy EU PSD2 Strong Customer Authentication (SCA) and dynamic linking requirements without exposing PII.

2.3 HID Approve

HID Approve is HID Global's transaction signing and authentication solution that uses push notifications. It can be fully integrated into the authentication platform, but is also available as a stand-alone application or as an SDK with minimal integration necessary to deploy.

The solution offers the strongest security protocols and cryptographic standards to secure consumer transactions. It helps secure channels with out-of-band communication that is protected by device-specific keys. No personal information is included in the push notification, which enables organizations to be compliant with data protection regulations around the world.

HID Approve also enables EMV 3D Secure for better protection built in for eWallets, online banking and mobile payments. HID Approve is part of the authentication platform which combines elements into a packaged service that is suitable for B2B, B2C, B2E and G2C use cases.

3 Strengths and Challenges

The volume and complexity of fraud is increasing, and businesses in almost every industry as well as government agencies are actively seeking Fraud Reduction Intelligence Platforms (FRIP) to mitigate these risks. FRIP solutions are designed to interoperate with transaction processing and authentication systems.

HID Global's Risk Management System has a number of competitive advantages beginning with a robust set of identity proofing features, including remote identity document verification and authoritative attribute lookups. Integration with ITSM, advanced bot management, and the ability to consume external sources of threat intelligence would be beneficial.

Having numerous government agencies as customers of their credential issuance products is a significant endorsement of the trustworthiness of their solutions. Furthermore, HID Global has obtained relevant security certifications for their products and services. The functional areas of device intelligence and behavioral biometrics are addressed by their secure mobile SDK and JavaScript. HID Global's micro-services-based and cloud-hosted infrastructure can scale as needed for demanding customers. Organizations looking for advanced fraud reduction with built-in identity proofing capabilities that utilize the latest high security crypto standards will want to consider the HID Global Fraud Prevention Offering.

Strengths

- Identity proofing and authoritative attribute queries supported out-of-the-box
- Strong credential issuance capabilities trusted by numerous government agencies globally
- Digital identity verification app
- Intuitive admin and fraud analyst interfaces
- Secure mobile SDK for device intelligence and behavioral biometrics, including innovative modalities
- UBA considers transaction level details
- Pertinent security certifications
- Incident response and site takedown services

Challenges

- Bot detection capabilities are present but advanced bot management must be handled in customer systems
- External sources of IP reputation, compromised credential and device intelligence would enhance the solution
- No connectors for ITSM systems

4 Related Research

Leadership Compass Fraud Reduction Intelligence Platforms (2021)
Leadership Compass Fraud Reduction Intelligence Platforms (2020)
Executive View HID Global Authentication Platform

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.