Overview

Satisfying increasing customer expectations has never been more challenging for financial institutions in a hyper connected world where intuitive experience and innovative digital services are re-shaping lifestyles. Digital Identity is becoming our passport through the digital world and therefore the need for financial institutions to protect it is urgent in order to safeguard customer’s trust and seize new growth opportunities while meeting the requirements of regulations such as PSD2, HKMA, FFIEC, etc.

HID Risk Management Solution allows financial institutions to mitigate the risks of even the most sophisticated cyberthreats whilst providing a seamless and optimised user experience. This paper outlines the benefits of implementing a threat detection approach and details the technical requirements financial institutions should look for when seeking an integrated layered authentication platform to ensure a consistent security experience for omni-channel banking.

The Problem: Maintaining Security in the Face of Increased Threats – While Balancing Access Requirements and Costs

Any financial institution or business that offers Internet and mobile banking, online financial services, alternative payment solutions or an e-commerce website is a top target for cyber criminals, due to the sensitive and potentially lucrative nature of the financial data transacted through those channels. They are likely to face targeted Man-in-the-Browser (MitB), trojans, viruses, phishing, social engineering, malware, malvertising, Remote Access Trojan (RAT) attacks and zero-day attacks as attackers try to execute fraudulent transactions that can often result in losses amounting to millions of dollars.

If customers connecting to banking applications are doing so via infected desktops, laptops or smartphones, the malware resident on these machines can spy on all their activity and collect sensitive information, including usernames and passwords. As a result, when customers conduct banking or other financial transactions, the attacker can perform an account takeover and capture critical information, such as physical address information, phone numbers, identity verification information (secret questions/answers) and account balances. In addition, they may also be able to gain complete control over any Internet sessions initiated from that enduser’s device, including Internet banking, online brokerage or other financial account service transactions (loan applications, credit card applications, etc.).

In most cases the victim remains unaware about an account takeover until money is stolen from their account. If fraudsters want to avoid detection they may choose to transfer a series of small amounts from the victim’s account which may go unnoticed taking into consideration that most of the accounts are paperless and only vigilant customers regularly check their on-line bank statements.
While financial institutions know they need to add security, they can’t afford to add time or complexity; they need a way to support all the access requirements of their customers, while appropriately balancing the customer needs, costs and security requirements of their business.

The Solution: How HID Risk Management Solution Works

1. Introduction

The HID® Risk Management Solution is a real-time solution that protects businesses against cybercriminals and helps organisations to validate valuable returning customers and prospects. It is a cloud-based or on-premise, cost-effective solution that uses risk profiling technology.

Digital payment and online services dangers are growing in terms of variety of attacks and their volume. The majority of detected threats use specialized tools in at least at one stage of the attack. Alongside malware driven attacks, there are ever more fraudulent schemes based on phishing, social engineering methods, attempts to misuse the application or to bypass the application business logic and limits.

Neither the traditional approach with solutions based on rules and transaction anomaly detection nor IP and browser-based user identification techniques are sufficient nowadays.

HID Global brings an alternative next generation online fraud and cyber threat detection solution able to detect traditional as well as modern threats that jeopardize online and mobile banking, transaction systems and sensitive applications. Our solution is a full-stack fraud detection system based on a modern cognitive security user centric approach. Combination of evidence-based cyber threat detection capabilities and behavioral biometrics supported by machine learning makes a perfect fit for combating the ever-changing threat landscape of modern banking applications.

In our efforts to provide financial institutions with the right solution, we propose the Fraud and Threat Detection modules for web-based internet banking application as well as mobile banking application protection:

- Unprecedented detection capabilities (zero-day banking malware, account takeover, phishing, fraudulent transactions, BOTs and more)
- User verification based on behavioral biometrics – seamless authentication
- Identify ongoing fraud attempt even before money is actually transferred
- Deployable in days compared to months long implementation project of traditional fraud detection systems
- Integration can be done without any API integration work
- Supports risk-based multifactor authentication
- Application usage and users activity monitoring for marketing teams
- Complies with regulatory rules and recommendations issued by the European Central Bank
- Fraud analyst and global intelligence network is proposed as a part of the service
2. Description of HID Risk Management Solution

HID Risk Management Solution uses Digital Identity Sensing Technology (DIST) to detect fraudsters amongst genuine users. DIST brings a unique set of device fingerprinting and user identification techniques and was developed because traditional fraud detection methods could not keep up with modern threats and complex digital environments. It relies on the fact that every user is identifiable by his or her behavior patterns, biometric markers and typical actions (including but not limited to payments). By analysis of such parameters using the latest Machine Learning and Artificial Intelligence technologies, we are able to detect minor changes on the user side and spot the fraud even in the creation phase, which was previously impossible.

DIST uses a layered approach - at each stage of the user interaction with the protected application, security checks are applied to detect differences in assumed identity. If the current profile differs from the learned model by certain customizable threshold, an alert is raised. One out of many advantages of the proposed solution compared to common Fraud Detection Systems is the ability to collect and evaluate in-session data (speed and timing of actions, user activity, user interaction with application and more). This greatly increases fraud detection chances as well as improving quality of information about the users of the digital service.

The following diagram shows the detection layers deployed by HID Risk Management Solution.

HID Risk Management Solution (RMS) is a complex anti-fraud system designed with modern fraud schemes and attack types in mind. Most of the capabilities of the RMS system are based on unique Device Fingerprinting and User Identification technology. This unique technology can serve financial institutions fighting against fraudulent transactions, fraudulent account signups, account takeovers or to simply gets more insight to who the users are and how they use the protected service.
What does HID Risk Management Solution do?

HID Risk Management Solution is a response to numerous requests from banks, online service providers, micropayment providers and other businesses where reliable user identification is the key security component in elimination of fraudulent service access attempts. This is combined with other threat detection features such as banking malware or transaction anomaly detection. It uses correlation of data from JavaScript or SDK probes working silently on a user's endpoints (no installation or interaction of any form with the user is required) and advanced machine learning and statistics. Our invented algorithm fingerprints every device and the user is monitored throughout the whole online session. In addition to mouse and keyboard biometrics, our solution also gathers information about the location, browser, IP addresses and typical behavior patterns of the user. When the user performs the payment or other financial transaction, HID Risk Management Solution already knows what is wrong and, if necessary, marks the fraudulent money transfer attempt with all the transaction relevant data. All data is gathered and analyzed in real-time making it possible to identify imminent attack at any point in time of the active session (session takeover for example).

Analytics interface providing actionable insights

HID Risk Management Solution comes with an Analytics interface for Fraud Analysts, System Administrators and Security Managers to be able to gain an overall view on the current security level of the protected frontend applications and an indication of imminent threats. All detected incidents are categorized and come with a myriad of sensitive information about the affected user, device, session or transaction. There is a case management system available to prioritize and group incidents into cases for various internal teams to work on. Scoring is provided for every user, device, session or transaction.
Conclusion

The risk levels of financial institutions and their customers are growing exponentially, due to highly motivated attackers who are applying increasingly sophisticated and targeted attack techniques to commit financial fraud. These attacks are compromising legitimate users’ desktops, laptops and mobile devices in a way that circumvents the traditional customer identification mechanisms deployed by financial institutions today, in order to steal information and conduct fraudulent transactions.

Staying ahead of these sophisticated attacks, mitigating institutional risk, and enabling trusted online transactions from any device or browser requires a coordinated, layered authentication approach.

To learn more about how our banking solutions can help provide you with continuous risk-based authentication and increase your protection from costly data breaches, visit us online at hidglobal.com/iam.