White Paper

BIOMETRIC SECURITY FOR SELF-SERVICE BANKING AND PAYMENT TERMINALS: WHEN GOOD ENOUGH IS *NOT* GOOD ENOUGH

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Lumidigm®
part of HID Global

First Edition January 2017

Sponsored by HID Global

Published by:
Goode Intelligence

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

This white paper from biometrics research and consultancy specialist, Goode Intelligence (GI) argues that some biometric authentication technologies may look attractive on paper but often do not provide adequate levels of user convenience, transaction security and system reliability, so they end up being expensive when viewed over the lifetime of service. It argues the case that to properly address identity related problems in self-service banking and payment terminals, one must deploy a biometric solution that provides both high levels of security and high user convenience and that the absence of either element increases the total cost of ownership.

Analysis and data has been drawn from a study undertaken by Goode Intelligence to understand the ROI of HID Global's Lumidigm® multispectral imaging fingerprint solutions.

DELIVERING HIGH SECURITY AND HIGH USER CONVENIENCE

In today's digital world, convenience is an important factor when choosing consumer-facing technology. Convenience is a hot topic in security and customer authentication. This is particularly so for financial services where the search for convenience, simplicity and sense of security are integral components of a modern omni-channel strategy.

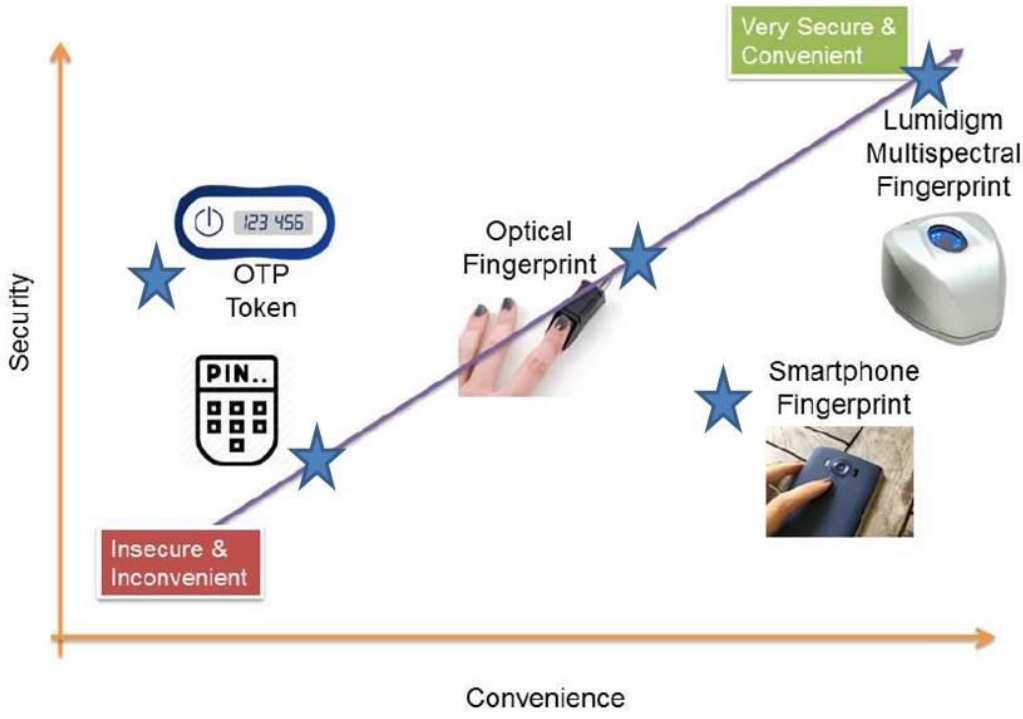
The balance between convenience and security can be a tough one to get right. Cumbersome security mechanisms adversely affect the convenience of banking services, so customers may simply choose to avoid the hassles and switch their service provider, resulting in lost business to the financial institution. Conversely, security mechanisms that are easy to use improve overall customer satisfaction ensuring a positive customer experience and increased adoption, helping businesses increase revenues from those services. Convenience is a critical component of a successful solution but it can never be at the expense of real security, especially in real world applications where malware and other threats steal millions of identities resulting in billions in financial losses to banks, retailers and consumers.

For instance, a smartphone-based fingerprint sensor, such as Apple's Touch ID, is a convenient use of biometrics for PIN replacement (although these sensors can be unreliable when a finger is wet or dry, leading to user frustration). However, biometric authentication with Touch ID and other mobile device-based fingerprint technologies do not offer the best in-class security and can be spoofed.

Ironically, most of today's billions of ATM transactions are also protected by just a four-digit PIN, which is neither convenient nor secure. OTP tokens may offer a higher level of security but are inconvenient in many physical world scenarios.

The bottom line is that many organizations are often forced to choose between convenience and security when implementing customer authentication solutions. The reality is that we should not be creating a false choice but rather looking for a no-compromise solution: one that is *BOTH* very secure and very convenient.

Figure 1. You Can Have Convenience and Security



Source: Goode Intelligence

TACKLING FINANCIAL FRAUD IN SELF-SERVICE BANKING AND PAYMENT TERMINALS

Financial fraud in self-service banking and payment terminals, including ATMs, is a global problem. Figures show that the number of incidents and losses from fraud at the ATM and point-of-sale (POS) terminals are rising.

Card skimming, PIN theft, card theft and the emergence of targeted malware are some of the threats that are sending financial fraud levels on an ever-upwards trajectory in all regions of the world.

2015 saw the highest levels of ATM fraud in Europe since 2008 with losses of almost US$370m[1]

[1] European ATM Security Team (EAST) https://www.european-atm-security.eu/files/Card-skimming-losses-continue-to-rise-outside-Europe-for-release-to-the-media-on-12th-April-2016-.pdf

Russian mafia are targeting tourists in Cancun, Mexico, using skimmers that broadcast card data using Bluetooth Beacon technology. An estimated $5 million per month in 19 compromised ATMs has been defrauded from ATMs that have been tampered by 'official' engineers who were bribed by Russian gangs to install the $500 skimmers[2]

Source: Krebs on Security

In keeping with our premise that biometrics solutions to such problems must be both secure and convenient, today there is a commercially available technology that dramatically reduces the risk of financial fraud in these scenarios while extending a good measure of usability and convenience to bank customers. HID Global's Lumidigm multispectral imaging biometric solutions are a proven method to reduce financial fraud in self-service banking and payment terminals. When several banks in Brazil replaced chip and PIN authentication with Lumidigm biometrics, fraud losses decreased by 52 percent from 2012 to 2015, saving millions of dollars.

Brazil: ATM fraud losses decreased by 52 percent between 2012 and 2015 when Lumidigm multispectral fingerprint authentication replaced chip and PIN [3]

Source: Nacho Doce/Reuters

[2] Source: Krebs on Security, https://krebsonsecurity.com/2015/09/tracking-a-bluetooth-skimmer-gang-in-mexico/
[3] Source: Biomatica - http://biomatica.com/

THE ROI OF BIOMETRIC IDENTITY VERIFICATION

After they carefully considered their business needs, security risks and need for improved customer usability, several top Brazilian banks made the decision to deploy Lumidigm fingerprint solutions from HID Global to address a pressing need for convenient and secure authentication mechanisms in self-service banking and payment terminals.

PIN-based authentication solutions had proven to be totally inadequate as they are neither convenient nor secure. They are also more costly to maintain and are ineffective in enabling other secure services, severely limiting the providers' ability to retain and acquire new customers.

Biometric sensors can provide a convenient alternative to PIN-based customer authentication, but not all biometric technologies or implementations can deliver a convenient solution along with fraud-reducing security. In a recent return on investment (ROI) study carried out by Goode Intelligence, it was found that a number of biometric sensors, including low-to-medium priced fingerprint sensors, did not match Lumidigm's solutions in a number of key areas. In short, the lower cost of these sensors did not result in better savings nor was the perception of security a substitute for real security. And these cheaper sensors did not deliver a more compelling multi-year ROI, despite their lower initial cost.

The study measured Lumidigm's popular V-Series sensors against a number of other biometric sensors with particular focus on key criteria that included the real ability to reduce financial fraud, user experience, support and maintenance costs, and total cost of ownership (TCO) — all while delivering security and convenience.

Key cost, reliability and fraud reduction factors were measured against both PIN-based and other biometric authentication solutions, and the Lumidigm multispectral sensors came out on top. And despite a higher initial sensor cost, the overall solution investments were actually found to be more cost effective over the typical lifetime of an ATM or self-service kiosk versus competing biometric devices.

MEETING THE CHALLENGE: LUMIDIGM BIOMETRIC SOLUTIONS

Lumidigm M-Series Lumidigm V-Series ***Source: HID Global***

The integration of Lumidigm V-Series multispectral fingerprint sensors into bank ATMs is one of the most successful commercial biometric authentication stories to date. In Brazil alone these sensors are being used by more than 85 million banking customers in over 85,000 ATMs, securing over 3 billion ATM transactions per year.

Both private and public sector banks in Brazil were faced with the challenge of dealing in a high-fraud environment. Over the past several years they replaced both PIN-based and competitor biometric solutions with Lumidigm multispectral fingerprint sensors because they are the only devices that meet banks' demanding requirements for strong transaction security, user convenience and high reliability operation. They are also the only biometric sensors proven to:

- Secure demanding self-service banking applications
- Speed customer transactions at ATMs and self-service kiosks
- Lower staff and maintenance expense.

Multispectral fingerprint imaging is ideal for these unattended applications because it was designed to capture surface and subsurface information using multiple wavelengths or colors of light from different angles, enabling it to work reliably for all people in "real world" applications like ATMs, self-service kiosks and payment terminals. Because traditional optical or capacitive fingerprint sensors only capture surface details of the finger, their usability is problematic under less than ideal conditions, resulting in higher customer frustration, especially if the user has wet, dry, dirty, worn or elderly fingers.

In addition to delivering better biometric usability, multispectral fingerprint imaging also offers another important advantage that makes the Lumidigm technology the best-in-class solution for liveness detection. Determining if the finger on the sensor is from a real live person or is a fake or stolen copy of a fingerprint is a task that multispectral imaging excels at. By contrast, spoofs easily defeat Apple's TouchID and other lower quality biometric devices.

Source: HID Global

Over 3 Billion ATM Transactions per year are secured using HID Global's Lumidigm multispectral fingerprint sensors

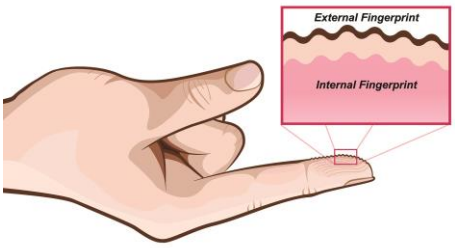
HID Global's range of Lumidigm biometric solutions are based on three core capabilities operating within a trusted or secure processing environment. They include:

1. **Capture**: A simple and repeatable user experience is essential in today's competitive consumer-driven market. The ability to reliably capture any user's fingerprint image in all conditions is essential. Banks should only deploy a solution that works for everyone everywhere, no matter if their finger is wet, dry, dirty, elderly, in bright light, hot or cold.
2. **Liveness**: The ability to detect that a presented finger is real and not fake is essential for trusting a biometric system. The U.S. National Institute of Standards and Technology (NIST) has recognised the importance of liveness detection as a vital part of a trustworthy biometric system, through its recommendations for Presentation Attack Detection (PAD). Multispectral imaging ensures that faked or stolen fingerprints will not work when presented at the sensor. This enables banks and payment processors to be confident that each person can use their own biometric — and no one else's — to authenticate their transactions, and that each customer's digital identity and personal privacy is protected.
3. **Match**: Fingerprint data obtained from Lumidigm fingerprint sensors provide proven match results and are interoperable with existing industry standards for fingerprint template databases, including ANSI 378 and ISO 19794-2 MINEX templates standards. Fingerprint matching is only meaningful after you accurately capture high quality biometric data and confirm that it is real, not fake.

Source: HID Global

The above three biometric functions must occur in a secure processing environment, to ensure the data is not tampered with during capture, liveness detection or the matching process. The Lumidigm multispectral fingerprint sensors provide a secure processing environment with certified cryptography and anti-tamper capabilities that prevent attacks such as man-in-the-middle and image substitution, resulting in improved trust. These attacks can easily defeat other biometric systems, exposing them to cyber-attacks and tampered biometric results, reducing trust and increasing the risk of fraud.

Lumidigm multispectral imaging captures surface and subsurface fingerprint data, for best-in-class usability and best-in-class liveness detection



Source: HID Global

SUMMARY

The bottom line is that in the world of secure financial transactions, there is a continuous struggle to balance real versus perceived security, while also delivering user convenience in a cost-effective way. This white paper explored this challenge in the context of mission critical applications like ATM cash withdrawals and other self-service financial transactions that require a higher-level of security and reliability to serve today's diverse and demanding customers. We determined that financial services and other organizations need not give up higher levels of security when designing user-friendly customer-facing services. Today, it is wholly possible to deliver both high levels of security and excellent user convenience. Financial institutions can have BOTH security and convenience; they are not forced to compromise.

The right technology is one that allows organizations to deploy reliable and cost-effective customer authentication solutions. They must operate reliably in all conditions with all people and be robust enough to establish the necessary trust that the person conducting the transaction is who they claim to be. When such a solution is deployed it has been demonstrated that financial fraud can be reduced by over 50 percent. When looking at the service life of customer-facing banking services like ATMs and payment terminals, the lowest cost biometric technology does not deliver the lowest total cost of ownership over the serviceable life of the system. Solution providers should look at a multi-year ROI and the fraud reduction capability of the technology when determining which solution to deploy.

HID Global has shown itself to be the proven leader in secure and convenient biometric authentication in demanding self-service applications, with more than 3 billion secure ATM transactions per year just in Brazil plus many other successful deployments in other regions of the world and for other applications and markets. This is the main reason why Lumidigm multispectral fingerprint imaging has become the technology of choice in demanding ATM, self-service and payment terminal applications. To learn more, read Biometric Authentication at the ATM.

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in mobile security, identity and biometrics. The company is the publisher of the '***Biometrics in Financial Services***' series of analyst reports that were first published in 2015 and offers a ***Biometrics Insight Service*** offering annual subscription to publications and advisory services.

For more information on this or any other research please visit www.goodeintelligence.com.