Trust but Verifi

Understanding Biometrics in Card-Not-Present Transactions

Many Card Not Present ("CNP") merchants want to better understand biometric authentication and the impact it will have on their business. In most cases, cost is no longer a barrier and the technology has become increasingly accessible, making adoption a real possibility for merchants looking to fortify security. What's more, consumers are on increasingly on board. With 12.6 million victims of identity fraud in 2012, privacy concerns are being overshadowed by the desire for increased payment security[1]. Biometrics has been used for many years in high security applications via eye scan, finger- and palm prints as well as voice recognition technology. Biometrics is now making its way into CNP payments as mobile commerce gains momentum and as the EMV mandate begins to take hold over the next several years. This article will discuss the implications of biometrics for CNP merchants.

What is Authentication?

Authentication is key to successful CNP commerce; recent breaches have exposed weaknesses in payments security and as EMV looms on the horizon, the need for airtight CNP authentication will only increase. There are three primary ways in which a customer can authenticate his or her identity[2]:

1. **OWNERSHIP FACTOR** – Something a person has, like a credit card or other physical token.
2. **KNOWLEDGE FACTOR** – Something the person knows, like a PIN or password.
3. **INHERENCE FACTOR** - Something the person is or does, like a fingerprint or unique facial features.

Technologists are focused on using inherence or biometrics for authentication.

The addition of biometrics (three-factor authentication) can ensure and protect the identity of the cardholder. The plus for biometrics is that they cannot easily be counterfeited as they are unique to the customer and they are easily accessible for the user. On the flip side, this type of authentication is less convenient for consumers and usually requires a longer time commitment for the checkout process as the merchant is requiring an additional factor of authentication. The following are some common forms of biometrics and their considerations for use in the CNP environment.

[1] *http://cardnotpresent.com/articles/displaylogin.aspx?id=5160*

[2] *http://www.emv-connection.com/wp-content/uploads/2014/01/CNP-WP-012414.pdf*

Types of Biometrics

TYPE	PROS	CONS	EXAMPLE
Digital Fingerprinting - utilization of a touch sensing device or scanner to capture a person's fingerprint image to which a live scan of the person's finger can be compared to gain access or entry.[3]	Convenient and growing authentication method – especially in newer smartphones	Not as common in other devices such as desktop and laptops	The iPhone 5s can be locked and unlocked by touching a fingertip to the device screen; this technology also allows Apple customers to authenticate on iTunes.[4]
Facial Recognition - Technology application that identifies 80 nodal points on the human face and compares these points to a digitally stored image to confirm the identity of a specific individual through pattern identification.[5]	Prevalence of digital cameras on mobile devices, laptops and desktops makes "pay by face" an accessible option.	May require use of specialized camera installation on devices; may require users to pay additional fees and may raise some privacy concerns over the storage of facial images in databases.[6]	Used in US-VISIT (United States Visitor and Immigrant Status Indicator Technology) to verify the photographs of foreign travelers attempting to gain entry to the United States against those submitted at the time of visa issuance.[7]
Voice Verification - Technology that compares a person's voice pattern to a previously recorded vocal biometric to confirm an individual's identity.[8]	Voice recognition technology is user-friendly (non-intrusive), relatively inexpensive and most computer systems have microphone capabilities built-in.[9]	Health and emotional state can cause variance in a person's speech, causing a mismatch between voice template and sample submitted for verification.[10]	The US PORTPASS Program uses voice recognition via handsets to identify enrolled local residents along the U.S.-Canadian border, allowing them to cross the border when the port is unstaffed.[11]
Iris Recognition - Technology that analyzes the random pattern of the iris to recognize and identify a person.[12]	Image of the iris can be captured using a standard camera and matching a person's iris with the stored version is highly accurate.[13]	The iris is difficult to scan from a distance and can be obscured by eyelashes or eyelids. There can be difficulty in reading the iris of people who have cataracts or are blind.[14]	Iris recognition is currently used for physical access control.[15]

[3] *http://www.businessdictionary.com/definition/digital-fingerprint.html*

[4] *http://cardnotpresent.com/news/cnp-news-may14/CNP_Expo__Are_Biometrics_the_Authentication_Answer__-_May_20,_2014/*

[5] *http://whatis.techtarget.com/definition/facial-recognition*

[6] *http://www.parl.gc.ca/content/lop/researchpublications/06-30-e.htm*

[7] *http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition4.htm*

[8] *http://www.transparencymarketresearch.com/voice-verification.html*

[9] *http://www.globalsecurity.org/security/systems/biometrics-voice.htm*

[10] *http://www.globalsecurity.org/security/systems/biometrics-voice.htm*

[11] *http://www.globalsecurity.org/security/systems/biometrics-voice.htm*

[12] *http://www.biometrics.gov/Documents/IrisRec.pdf*

[13] *http://www.sans.org/reading-room/whitepapers/authentication/iris-recognition-technology-improved-authentication-132*

[14] *http://www.sans.org/reading-room/whitepapers/authentication/iris-recognition-technology-improved-authentication-132*

[15] *http://www.irisid.com/currentfutureuse*

While some privacy concerns do exist over the storage and use of biometric information, consumers appear willing to set aside privacy concerns for heightened CNP security.

Findings show that 49% of consumers are ready for biometrics.[16] A recent white paper by Nicole Reyes of The Members Group published noted that 51% of consumers surveyed had concerns over a company or mobile device having access to their fingerprints[17]; however, that number may drop as additional methods of storing data are researched, such as only storing the information on the consumer's payment card.

While use of biometrics to many may seem like "big brother is watching", consumer sentiment may be shifting and allow for faster adoption. A recent Associated Press poll pointed out that 58 percent of consumers have "deep concerns" about their personal data in online transactions,[18] signaling that they may be more open to added security measures like biometrics. Mass adoption of biometrics as a security tool may still be off in the distance, but CNP merchants should consider utilizing biometrics as a tool that is part of a comprehensive risk and evolving fraud management strategy. Staying on top of all the available technology and tools in a layered approach will allow CNP merchants to keep up with the fraudsters and guard against new threats without damaging the customer experience.

[16] *http://www.infosecurity-magazine.com/view/22732/mobile-wallets-and-mbanking-how-secure-are-they/*

[17] *http://www.tmgmktg.com/WP/TMG_wp_BiometricAuthentication_FINAL.pdf*

[18] *http://cardnotpresent.com/news/cnp-news-jan14/Report__U_S__Consumers_'Concerned'_about_Breaches,_But_Not_Showing_It_-_Jan__30,_2014/*

VERIFI™

For More Information

Main Phone: (323) 655-5789   Mon-Fri 8:00 AM – 5:00 PM PST
Main Fax: (323) 655-5537
Email Address: info@verifi.com

Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048