Burrus Research®

## Will Biometric Logins Replace Your Passwords?

Bank notes and silver coins are starting to feel incredibly primitive or quaint at best to an increasing number of shoppers. Many are happier using their credit or debt card for both their online and offline purchases. Now that the U.S. has joined Europe and other nations by requiring a chip-in-card system, the pressure is on technology to increase security and at the same time replace other annoyances from our past such as PINs and the dreaded passwords.

An estimated 53% of us forget crucial passwords more than once a week. Does this sound familiar to you? These forgetful episodes often involve us losing more than 10 minutes that we will never get back as we embark on the cumbersome reset of our account process. This often leads to shoppers abandoning their purchase through sheer frustration, while others miss out on buying concert tickets to a show that sells out in record time.

With our login details written down on pieces of paper or notebooks, there is also a serious security issue that needs addressing. The road to progress involves improving the current process by making life simpler for consumers while also increasing security to prevent hacking or loss of personal data.

I have been writing about the use of multiple biometric identification as a more secure method of authentication. Despite many thinking this technology would be nothing more than Hollywood fantasy, Apple's latest smartphone changed that for the masses when it introduced both biometric identification and its Apple Pay system using tokenization. In an effort to keep credit cards from fading into history, MasterCard recently announced that they were beginning a phased launch of the first biometric corporate credit card program across Canada and the U.S.

This technology will enable cardholders to verify transactions using facial recognition and fingerprint biometrics when making online purchases. The ethos of both Apple and MasterCard is that consumers shouldn't have to sacrifice convenience for security. Each and every one of us is unique, so what could be more secure than enabling the person to become the password?

The concepts of taking a selfie or scanning a fingerprint to authenticate our bank account is no longer an expensive or controversial idea. Amazon also hit the headlines recently after filing a patent that would enable its customers to pay by taking a selfie. Only 12 months ago, many would probably have scoffed at such a suggestion, but as I have pointed out in previous articles, the military has been using facial recognition for some time now with great success.

A few weeks ago, mobile payments technology stole the show at the Mobile World Congress (MWC) in Barcelona. Swiping or tapping our way through checkouts using wearables or even smart clothes seemed to promote the idea that nothing is impossible, and that there is no such thing as a bad idea.

The Visa Token Service (VTS) offers a slightly different approach to the future of payments by replacing the 16-digit credit card number with a unique digital identifier that can be placed inside wearables, clothes, and appliances through the obligatory Visa Ready partners.

When looking at the future of mobile payments, digital wallets often dominate conversations, but our future offers much more than smartphones with Touch ID. It has recently been estimated that one billion users will access banking services through biometric systems by 2017. If this prediction comes to fruition, we can expect an incredible level of growth in the biometrics industry.

The success of this technology will largely depend on user adoption rates and if they are ready to embrace a digital world where they pay for items with a fingerprint and/or a selfie, as well as adding their voice and heartbeat pattern—to name a couple more proven biometrics—when additional security is needed. When MasterCard launched its first worldwide pilot of this technology in Holland, it discovered the overwhelmingly positive news that nine out of 10 participants reported they would like to replace their password with biometric identification.

The pilot users interestingly highlighted how users preferred fingerprints and facial recognition authentication to the out-of-favor passwords. This suggests that adoption of this new way of authenticating will not be as difficult as some believe.

Physical cash, PINs and passwords are all beginning to look a little dated. It shouldn't be too much of a surprise to see multiple biometrics being embraced by both users and businesses. It appears that the biggest dilemma coming our way in the near future will be if we will use a smarter credit card or have all our cards in a smarter smartphone. What would you prefer?

**About the Author:**

**DANIEL BURRUS** is considered one of the world's leading technology forecasters and innovation experts, and is the founder and CEO of Burrus Research, a research and consulting firm that monitors global advancements in technology driven trends to help clients understand how technological, social and business forces are converging to create enormous untapped opportunities. He is the author of six books including The New York Times best seller Flash Foresight. This article is reprinted with permission. Reproduction without permission is strictly prohibited. For reprint permission, contact Burrus Research, Inc. at office@burrus.com.

INOVA BUSINESS SCHOOL

INOVA CONSULTING