Learning at Third Level Assignment 2 Review – Group Project-New Idea

Assessment of Similar Products of Biometric Payments on the Global Marketplace

Jack Carroll

T00194823

Contents

[Introduction 3](#_Toc466909288)

[Assessed Technologies 4](#_Toc466909289)

[Technology 1 4](#_Toc466909290)

[Technology 2 5](#_Toc466909291)

[Technology 3 6](#_Toc466909292)

[Conclusion 7](#_Toc466909293)

[References 8](#_Toc466909294)

# Introduction

The amount of biometric payment products that are present in the technology sector is rapidly increasing due to the preparation of consumers to use biometric methods for making payments. According to a research project carried out by Visa, three quarters of consumers are becoming familiar with the “two-factor authentication” in biometrics, i.e. fingerprint scanning where a payment device can collaborate with biometrics to allow the products to become more functional (Anonymous, 2016). Three technological advancements in the biometrics market that could revolutionise the way in which millions of citizens pay their bills and taxes are assessed here for inspiration and for the purpose of analysing similar products in the global market for “ThumbCash” to thrive.

# Assessed Technologies

## Technology 1

The first technology to be assessed in relation to biometric payments is an authentication application by MasterCard that requires a user to take a “selfie” to carry out payments. The “MasterCard Identity Check” process can validate an online payment by using the smartphone’s camera to identify the face for confirmation. Lomas states the global demand for this innovative scheme as the application is being introduced across Europe in various countries including Germany, Spain and the Netherlands. Eventually, the “Identity Check” app will be available from the start of 2017 as it assists fingerprint biometrics where users will be able to choose whether the finger or the face will verify the mobile payment when purchasing a product. This procedure has an advantage of eliminating the requirement of memorising passwords for online shoppers or for user bank accounts (Lomas, 2016).

## Technology 2

Another product that is becoming commercial in the biometric payment technology industry is the “Apple Pay” payment application that is available on “Apple” devices which includes the “iPhone” and “iPad”. This type of biometric payment is embedded in the “Wallet” app where the phone or tablet protects any card whether it is a debit card or credit card from being stolen physically. For the “iPhone” to authenticate itself in “Apple Pay”, the phone requires the home button to be pressed and the fingerprint to be scanned. To prepare the phone for usage of “Apple Pay”, the card must be added and permitted to carry out future payments. Ritchie clearly explains that numerous credit and debit cards are utilised because these cards can easily be changed when a “transaction” is performed (Ritchie, 2016).

## Technology 3

A third type of biometric technology that is popular worldwide based on its product is the recognisable payment application “Zwipe”. Chowdhry states how “Zwipe” collaborated with “MasterCard” to form the first ever credit card to combine biometric confirmation with “contactless payment technology”. For security purposes, the “Zwipe MasterCard” keeps the user’s fingerprints as this identification is a replacement for PIN number entries. This is useful as “payments of any amount” can be carried out where no prepaid amount is needed. The functionality of the card is simple for consumers as the near field communication installed in the card enables the user to signal it at terminals that are well-matched with the card. To improve the card’s capabilities, Chowdhry gives details about the updated version of the “Zwipe MasterCard” as the global consumers can use the card on all payment terminals. As well as this, the card can collect energy from the terminals, so therefore, a battery is not required for “future versions” (Chowdhry, 2014).

# Conclusion

It is evident that the products that are available globally for biometric use is steadily increasing due to the frequent usage of smartphones and tablets by the majority of the world’s population. These products are all successful as innovation is central to the creation of new services for biometrics. “Thumbcash” has a likelihood of succeeding in appealing to those with a bank account or who need to pay taxes as it would become efficient for the payment of money through a fob.

# Opportunities and Threats for “ThumbCash”

## Threats

According to the survey results that the group received for the idea of “ThumbCash”, the majority of respondents refused to use a thumbprint scanner if it was available as it is possible that thousands of people are afraid that personal details will be exposed due to the DNA of the fingerprints that would be taken from the scanner. Since the companies who produce biometric products require the information and details of the users, there is a fear that security and privacy protection could be a major threat for biometric systems because hackers and thieves could permanently steal the fingerprints and the iris through the use of tampering with the DNA of the user as fingerprints can easily be stolen for identification and easy access to the users’ personal details. These hackers could also “breach” confidential data of individual irises and fingerprints which were previously scanned (Gartland, 2016).

Another danger that is posed by biometric companies is the collection of biometric data that contains the history of scans by individuals worldwide according to Chickowski. The author explains that the details of the “biometric information” is unalterable which could lead to the misuse of personal data from the fingerprints and irises by hackers if the businesses do not find a solution to protect the privacy of the consumers when making payments with biometrics. Unfortunately, the user may never know that the personal data of the person is being gathered as the information becomes easier to collect. Thus, the risk of having intimate data being exposed by data breaches when biometrics scanning is being carried out is the primary reason why the “ThumbCash” group’s results revealed that numerous individuals did not want to use a fingerprint scanner if it was obtainable (Chickowski, 2016).

## Opportunities

Fortunately, the survey surprisingly revealed that although users would not be keen on using the “Thumbcash” device, a vast number of respondents answered that these users would probably carry out payments once a day or once a week which could prove that consumers are intending to gain an advantage from biometric payments. On reason that consumers would be prepared to use a fingerprint scanner for authentication is because of the potential for easier accessibility where updated technology would enhance the user’s experience. For example, if an individual was to leave the laptop unguarded when the user’s face allows the laptop to log in, the laptop can lock the screen instantly until the user who is currently logged in returns. This results in the laptop unlocking the system immediately which keeps the technology secure (Rosenquist, 2016).

# References

# References

Anonymous, 2016. *European consumers ready to use biometrics or securing payments.* [Online]   
Available at: https://www.visaeurope.com/newsroom/news/european-consumers-ready-for-biometrics  
[Accessed 14 November 2016].

Barris, M., 2014. *Samsung, PayPal tap fingerprint technology in smartwatch response to Apple.* [Online]   
Available at: http://www.mobilecommercedaily.com/samsung-paypal-tap-fingerprint-technology-in-smartwatch-response-to-apple  
[Accessed 14 November 2016].

Chickowski, E., 2016. *Enterprises Must Consider Privacy Concern For Biometrics.* [Online]   
Available at: http://www.darkreading.com/vulnerabilities---threats/enterprises-must-consider-privacy-concern-for-biometrics/d/d-id/1325501  
[Accessed 27 November 2016].

Chowdhry, A., 2014. *MasterCard And Zwipe Unveil Credit Card With Fingerprint Scanner.* [Online]   
Available at: http://www.forbes.com/sites/amitchowdhry/2014/10/18/mastercard-zwipe-fingerprint-sensor-credit-cards/#51c7ce9d6be1  
[Accessed 15 November 2016].

Gartland, C., 2016. *Biometrics Are a Grave Threat to Privacy.* [Online]   
Available at: http://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy  
[Accessed 27 November 2016].

Lomas, N., 2016. *Mastercard launches its 'selfie pay' biometric authentication app in Europe.* [Online]   
Available at: https://techcrunch.com/2016/10/04/mastercard-launches-its-selfie-pay-biometric-authentication-app-in-europe/  
[Accessed 14 November 2016].

Ritchie, R., 2016. *Apple Pay:The Ultimate Guide.* [Online]   
Available at: http://www.imore.com/apple-pay  
[Accessed 15 November 2016].

Simonite, T., 2014. *3 Things we learnt from Visa's.* [Online]   
Available at: https://www.technologyreview.com/s/525996/pay-with-your-fingerprint/  
[Accessed 15 November 2016].