Decision Support Systems xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment

Obi Ogbanufe [a], Dan J. Kim [b,*]

[a] Department of Information Technology and Decision Sciences, College of Business, University of North Texas, Denton, TX 76201, USA
[b] Department of Information Technology and Decision Sciences, College of Business, University of North Texas, 1307 West Highland Street, Denton, TX 76201, USA

ARTICLE INFO

Article history:
Received 14 January 2017
Received in revised form 13 November 2017
Accepted 13 November 2017
Available online xxxx

Keywords:
Fingerprint-based biometric authentication
Electronic payment
Security concern
Convenience
Usefulness
Trust

ABSTRACT

Biometrics authentication for electronic payment is generally viewed as a quicker, convenient and a more secure means to identify and authenticate users for online payment. This view is mostly anecdotal and conceptual is nature. The aim of the paper is to shed light on the comparison of perceptions and beliefs of different authentication methods for electronic payment (i.e., credit card, credit card with PIN, and fingerprint biometrics authentication) in an e-commerce context. As theoretical foundation, the valence framework is used in understanding and explaining the individual's evaluation of benefit and risk concerning the payment methods. We propose a research model with hypotheses that evaluate and compare the individual's perceptions of the payment authentication methods, trust of the online store, and the willingness to continue using the website account associated with the payment authentication method. An experiment is used to test the hypotheses. The results show that biometrics authentication significantly influences the individual's security concern, perceived usefulness, and trust of online store. Theoretically, through the study's context – biometrics versus credit card authentication – evidence is provided for the importance of the individual's perceptions, concerns, and beliefs in the use of biometrics for electronic payments. Managerial implications include shedding light on the perceptions and concerns of secure authentication and the need for implementing biometrics authentication for electronic payments.

1. Introduction

Recently, financial technology also known as FinTech is seen as an innovation that is poised to bring a new paradigm in financial services. Electronic payment solutions (e.g., digital wallets, Apple pay, and Samsung pay) are key FinTech applications. The electronic payment association notes that automated clearing House (ACH) volume grows to higher than 25 billion payments [1], translating to $43 trillion in electronic payment transfers in 2016. This growth is 5% >2015 and the third consecutive year where the volume grew by 1 billion over the previous year. Of this volume, online payment accounted for 23% of the ACH volume, growing 12% in 2016 with 4.6 billion web transactions. Considering its important role in the application of FinTech and e-commerce [2,3], the topic of electronic payment systems is of interest to researchers and practitioners. Electronic payment refers to payments made using a form of information and communication technology [4], and can include credit card, debit card, mobile payments, and web payments. Electronic payment continues to play an important role in the future of financial technology and e-commerce [5], and is more so given the increased adoption of mobile devices (e.g. smartphones, smartwatches, tablets etc.).

In spite of this growth, questions of security and privacy remain central in the adoption of electronic payment systems. Abrazhevich [5] suggests that traditional electronic payment systems have some limitations in the e-commerce context. FinTech experts suggest that traditional electronic payment such as PIN and chip based credit cards are flawed in its security protections [6]. Depending on the security of transmission and storage of information, these methods of payment and authentication become a target for cybercrime, which raises security concerns [7]. There are multiple occurrences of security breach events where credit card information and personally identifiable information are stolen or compromised from the payment and financial organizations (e.g. Heartland). The stolen information is often used fraudulently to open up new credit or bank accounts [8], which can cause psychological harm [9] and financial loss to the customer.

Biometric authentication for payment has been suggested as an alternative to traditional payment authentication methods [10]. Indeed, FinTech experts recently predict that traditional electronic payment such as PIN and chip based credit cards will eventually be replaced with mobile and biometrics authentication based payment [6]. A biometric is the automated use of unique human physiological or behavioral characteristics to determine or verify a person's unique identity [11].

* Corresponding author.
E-mail addresses: obi.ogbanufe@unt.edu (O. Ogbanufe), dan.kim@unt.edu (D.J. Kim).

https://doi.org/10.1016/j.dss.2017.11.003
0167-9236/

Authentication is the verification or validation of a person's identity [12]. Authentication determines whether individuals are who they say they are. Examples of traditional authentication methods are password, PIN (Personal Identification Number), and/or a token-based (e.g., card) authentication. Though biometrics technology is not new, there is no doubt an increase in its application and awareness made popular by mobile device manufacturers' inclusion of the biometric fingerprint technology in mobile devices. In addition, payment systems like PayPal have integrated their mobile applications with phone manufacturers' biometrics authentication to allow faster authentication for online purchases. Mobile device releases from Apple and Samsung have also made biometrics authentication a mainstream consumer technology. This presents a major boost in m-commerce, giving individuals the ability to complete online purchases via smartphones or smartwatches.

For individuals, some of the biggest benefits of using biometrics authentication include increased safety and security, and the reduced risk of losing their credit cards, having them stolen or used by others [10]. The rise of biometric authentication for payment has been linked to lower security concerns (e.g. preventing identity theft) and increased convenience [13,14]. These benefits can only be recognized with a wide deployment of biometrics authentication for payment. Indeed, about 770 million biometric authentication apps are projected to be downloaded annually by 2019 [15]. The need to improve these benefits is evidenced by the growing number of business services providing biometric authentications for electronic payment and other services [16]. Several conceptual papers that note the advantages of biometrics authentication over other types of authentication [17,18], also support it. Furthermore, biometrics authentication challenges such as security and privacy are important to individuals. According to Accenture [19], individuals are concerned about the capture and use of biometrics data, noting that these concerns determine the adoption of biometrics solutions for authentication. A survey of individuals reveals that 90% of respondents are concerned about data privacy with biometrics authentication [20]. Collectively, these observations indicate a need to investigate the perceived benefits of biometrics authentication for electronic payments, as well as the concerns over the security and privacy of the data collection and use of their financial data. Specifically, we seek to examine its perceptions in comparison with other payment authentication methods in order to inform our understanding of and to consider its adequacy in light of today's cybersecurity threats.

As is common in the implementation and use of systems designed to increase security, the tug between security and convenience becomes imminent. As systems become more secure, the less convenient they are perceived by users. For example, requiring users in an organization to change passwords [21] every month may increase security, but may be perceived as inconvenient by users. Given that trust has been seen as an important factor in online transactions [22–24], we also examine the individual's trust of the online store. The notion is whether individuals using biometrics authentication trust the online store more so than those using traditional payment authentication methods. Despite the influx of awareness and the use of biometric systems for authentication in electronic payment, systematic and theoretical research pertaining to the analysis of perceptions is limited. Studies on user perceptions about biometrics authentication in comparison with other authentication methods in e-commerce are scant.

Considering security, convenience, and usefulness as important valence elements of payment authentication methods, this study aims to investigate the issue by answering a research question. *How does biometrics authentication* versus *traditional electronic payment authentication methods influence (1) individuals' perceptions in terms of convenience, usefulness, and security concern, and (2) outcomes in terms of the individual's trust of the online store and their willingness to continue using the website account associated with the authentication method?* Given the influx of awareness and applications supported by mobile device biometrics, we are interested in examining whether biometrics in comparison with other payment authentication methods for electronic payment is perceived as safer and more convenient.[1] Considering the benefit and risk aspects of payment authentication methods, the valence framework is employed to understand and explain the individual's evaluation of benefits and risk. Valence is defined as the degree of positive or negative feelings toward a certain option [25].

Using an experiment, the primary interest is to assess individuals' perceptions and concerns of different authentication methods – fingerprint-based biometrics, credit card only, and credit card + PIN – in terms of their security concern, and perceptions of convenience and usefulness. The secondary interest is to examine the effect of the authentication methods on the individual's trust of the online store and their willingness to continue using the website account associated with the authentication method for future purchases.

Our findings suggest that security is a major concern, and that individuals do consider biometrics authentication more secure than credit card only (or credit card + PIN) authentication. This study has research and practical implications. First, by focusing on comparing fingerprint-based biometrics authentication versus traditional authentication methods, it is the first study that seeks to compare and understand how individuals perceive the security of payment authentication methods for e-commerce payment in IS research. With the prevalence and severity of security breaches resulting from e-commerce authentications (e.g. Equifax), this research raises awareness to the need for secure authentication in e-commerce transactions. Second, by focusing on the security, convenience, and usefulness aspects of the payment authentication methods, we contribute to the validation of the valence framework. Based on our literature review, we found that there are no empirical studies that evaluate and compare consumers' security concerns of different authentication methods for electronic payment in an experimental setting. Sensitivity to contexts is important, as it helps us derive meaning and understand the limits of generalizability [26]. Since this is a context that is becoming more important as electronic payments (including biometric authentication methods) continually grow, the empirical results of the study provide practical insights. We suggest insights that we expect will encourage the use of biometrics authentication in electronic payment applications.

In the next sections, we first provide an overview of electronic payment and biometrics literature, and then introduce the theoretical foundation of the study followed by the research model and hypotheses. Next, we discuss the research method, data analysis, and results. At the end of the paper, we present our findings and conclude the study by discussing implications for research and practice.

2. Literature review

It has been suggested that traditional electronic payment systems have some limitations in the e-commerce context, especially because of its susceptibility to cybercrime which raises security concerns [5,7]. This opens the door for biometrics authentication as a viable option for traditional electronic payment authentication. Prior studies have examined and compared traditional payment systems (credit card, money order, etc.) [27,28] in terms of protection, cost, and convenience. However, the focus of the current study is on the authentication methods used for payments in online transactions (e.g. biometrics, PIN, credit card authentication).

Over the last four decades, systems that provide biometrics authentication have been discussed in the information systems (IS) and security literature. Some discussions raise questions as to whether the technology is mature enough to offer the level of authenticated security required by industry. Others claim that recent developments of biometrics authentication have led to security enhancements of biometrics and that biometrics methods of authentication are less cumbersome and

[1] Although there are several different biometrics authentication methods such as fingerprint-based, iris, voice, face-recognition, etc., in this study, we focus on a fingerprint-based biometrics authentication.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

less subject to loss [29]. Thus, increasing its potential for e-commerce/m-commerce payments than traditional authentication and payment methods.

Biometrics technology has been used in many applications and industries such as in banking and finance (e.g., for the authentication of users to access safe deposit boxes), in manufacturing/commercial (e.g., for time and attendance recording), in law enforcement (e.g., for identifying suspects during crime investigation), in healthcare (e.g., for patient identification), and in border and national security (e.g., border entrance and immigration). Biometrics information is said to be unique, not easily forged like a signature, stolen like a password, or lost like a card [30]. A common concern for these applications is that biometrics data could be used for purposes other than what the individuals that provided their biometrics information intended for its use.

Several researchers have examined the determinants of biometrics adoption [31–34]. In these studies, the authors suggest that adoption of biometrics authentication is based on factors such as perceived usefulness, ease of use, risks and benefits. These studies also suggest that effort specific and benefit factors for biometrics use include cognitive effort saving, time convenience, and perceived enjoyment [31]. System attribute factors such as biometrics novelty [35], physical invasiveness [32,36], and personal factors such as innovativeness [33,34] and computer self-efficacy [34] are found to influence attitudes and intention to use biometrics based devices. Risk and trust factors concerning biometrics technologies are assessed for understanding their overall impact on use intention [33,34,36]. Risk factors such as security and privacy concerns related to the technology are examined to understand the individual's beliefs [37]. Previous studies have incorporated different biometrics modalities and contexts including biometric hand-scanner technology, fingerprint biometrics at ATMs [31,36], retina and iris scanning [32,33]. See Appendix A for a summary of biometrics adoption review.

2.1. Biometrics authentication for payment

Although biometrics technology is not new, research that examines the factors that affect the use of biometrics authentication in electronic commerce or mobile commerce are largely descriptive. There are few theoretically grounded studies that focus on the determinants of users' perceptions of biometrics authentication. Most extant literature provides descriptions of biometrics technologies, its architecture or viability [38]. Today, biometrics technology seemingly enjoys a wider acceptance due to the inclusion of fingerprint biometrics and more user-friendly applications on mobile devices. Security and trust are key concepts identified in the biometrics literature.

2.1.1. Security

Biometrics authentication involves the measurement and comparison of a person's features to a stored copy of the biometrics data. The goal of the authentication is to ensure that the biometric data captured at the point of authentication matches the previously stored version. Biometrics provides verification and identification features. Verification is when a person's identify is confirmed by comparing data stored on a document against the persons' identity, whereas identification is comparison and matching a persons' biometric measurement with the stored version. Traditional user authentication has either been based on something that a person knows (pin, password etc.) or something a person has (key, token smart card etc.) which have limitations and are prone to being forgotten or lost [39]. See Table 1 for the comparison of different authentication methods.

Some advantages of using biometrics for authentication include; (1) it reduces fraud, whereas prevailing approaches like username/password/PIN can be illicitly acquired by direct observation and then repudiated [40], it provides more accurate and reliable user authentication; (2) remembering passwords and PINs are no longer required, and (3) impersonation of identity is less of a problem. Other benefits of biometric authentication include the detection of illegal online account sharing of applications through keystroke analysis [41]. Prior research highlights the use of keystroke biometrics to detect when users share single accounts to circumvent fees, thereby defrauding the service provider. The study concludes with biometrics as a viable solution for user authentication and security administration [41].

Table 1
User authentication methods.
Adapted from Ratha, Connell and Bolle [40]

Method	Examples	Properties
What a person knows	UserID, password, PIN	Sharable, forgotten, easy to guess
What a person has	Cards, badges, keys	Sharable, duplicated, lost or stolen
Personal uniqueness	Fingerprint, iris, voice, iris	Not shareable, forging difficult

Though this view is mostly anecdotal, conceptual in nature and lacking empirical validation in IS literature, security is generally seen as the value proposition for biometric authentication's positive evaluation and subsequent adoption. In IS research, security is viewed as a key risk and major determinant of adoption [32,36]. Biometrics arguably provides a more secure alternative for authentication than traditional means, and this enhanced security can lead to the breakdown of trust barriers in online transactions [11]. Biometrics has been suggested as a technological deterrent to security risks, especially for the prevention of identity theft and false authentication in e-commerce transactions [42]. In spite of how secure biometrics is deemed, its effectiveness depends on (1) if the verifier can verify that the biometrics came from the person at the time of verification, and that (2) the biometrics matches the master biometrics on file [43]. A breakdown in either of these functionalities could present security issues. Even though the use of biometrics authentication has been proposed for curtailing security attacks, it is still susceptible to data breaches, as well as regulatory, legal, and operational challenges [44].

Sometimes, an overlooked aspect of biometric security is the challenge of protecting the individual's biometric templates when stored remotely or in a mobile device. Breebaart, Yang, Buhan-Dulman and Busch [45] identified a type of security threat targeted at storage systems, called storage subsystem threat. This is the illegal access or tampering of biometric storage systems, which could have cascading security and privacy ramifications. Issues with compromised templates could result in the loss of a user's identity. Tao and Veldhuis [14] tested the vulnerability of transmitting biometric data through a network and storing biometric templates on a database using face recognition biometrics authentication on mobile devices. They concluded that it is more secure, more convenient, and a cost-effective authentication method. With more biometrics applications emerging to meet the growing trend in biometrics authentication [46], and as biometric storage solutions expand to include cloud based biometrics authentication systems, so do the questions surrounding the security of such systems. Cohn [47] in a survey identifies that 92% of UK consumers and 69% of US consumers prefer that banks, credit card companies, healthcare providers and government organizations adopt biometric technologies, as compared to other protection measures such as smart card readers, security tokens or passwords/PINs to safely verify their identities. This number signifies a growing number of users who recognize the need for more secured methods of authentication. Thus, this calls for the gap in theoretically grounded literature that explores and seeks to understand security perceptions of biometrics to be filled.

2.1.2. Trust

Kleist [11] notes that biometrics technologies are poised to replicate the richness of human trust to a greater degree than other security technologies. Technologies, especially security enhancing technologies can engender feelings of trust in online environments and increase vendor

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

legitimacy. In online transactions, trust between the consumer and the vendor relies on the use of trust building electronic systems that identify and authenticate that individuals are who they say they are [48]. Biometrics authentication is a security technology that provides such authentication, which when used in e-commerce transactions can lead to trust in online transaction. From the online store's perspective, there is an assurance that customers are who they say they are. From the customer's perspective, which is the focus of the current study, s/he can have reasonable assurance that the online store makes an effort to keep their information safe and protected from identity theft or credit card fraud [11,49]. A recent survey of individuals in the US and Europe found that 65% of German and 46% of US consumers do not trust online firms that rely only on usernames and passwords for authentication [16]. In other words, consumers tend to trust online firms and websites that provide stronger authentication procedures. Though trust has been shown to be a critical factor in online transactions [50–52], few biometrics studies discuss trust as an outcome of biometrics use. The studies that do [e.g., [33,36]] only dealt with trust from the perspective of the performance of the biometrics system and the trust of the technology. As e-commerce and m-commerce technologies evolve, the focus shifts from building consumer 'trust in technology' to building 'trust in online vendors' [53]. Although Whitley, Gal and Kjaergaard [54] outline trust as a challenge in user identification and authentication, this study was mostly descriptive. Thus, there is need for in-depth empirical studies on biometrics use and its relationship to trust.

On the basis of the above review, we draw a few conclusions: (1) most literature on authentication methods including biometrics is conceptual in nature, lacking empirical analysis and theoretical foundations, and (2) the research on biometrics authentication is separate from research on traditional payment systems. We did not find research that integrates and compares biometrics authentication with traditional payment authentication methods in an e-commerce context, and none that compares on the basis of security and convenience.

3. Theoretical foundation

In order to depict how individuals evaluate the risks and benefits of using different payment authentication methods for online purchase, we use the valence framework as the theoretical basis of the study. Valence is defined as the degree of positive or negative feelings toward a certain option. The literature on valence framework [55] posits that perceived risk and perceived benefit are two fundamental aspects of consumer decision making. On the positive and perceived benefits angle, consumers are motivated to maximize the positive aspect, while the negative and perceived risk angle presumes that consumers are motivated to minimize the negative aspects. An extension of the valence framework is referred to as net valence. Net valence is the difference between anticipated positive and negative valence and suggests that individuals may attempt to maximize their net valence [55]. It implies that individuals' evaluations are characterized by both positive and negative attributes. Therefore, individuals will make decisions that maximize the net valence [56]. The valence framework provides the explanation that individuals will evaluate both the risks and benefits as they consider a certain option. In this study, individuals form perceptions of a payment authentication method based on its positives such as convenience, usefulness, time savings, and less cognitive effort. On the other hand, the individual may also consider the consequences of a security risk that might compromise their privacy, therefore leading to a negative evaluation. The risks and benefits valence are further elaborated below.

3.1.1. Perceived risk

There are numerous studies on the concept and impact of perceived risk. Perceived risk has been defined as the probability of loss in the pursuit of an outcome [57], as the expectation of loss and an inhibitor to intention [58], and as an individual's expectation of an unwanted outcome during or after an online transaction [59]. Recognizing that the risks under an individual's contemplation are multi-dimensional (e.g. perceived risk of product and perceived risk of transaction) [59], the current study deals with one of the two dimensions - perceived risk of transaction. The payment authentication method (credit card, credit card + PIN, or biometric authentication) constitutes the perceived risk of transaction, which includes the security risks associated with the payment method used in the transaction. In general, security risk is the potential for an individual's personal information to be viewed or altered during transit and storage by unauthorized personnel in a manner inconsistent with an individual's expectations [60], industry security guidelines and requirements. In this study, we focus on the individual's security concern for the payment methods.

3.1.2. Perceived benefit

Each electronic payment authentication method possesses specific benefits over their alternatives. Biometric authentication possesses several benefits that can be categorized as pre-transaction and post-transaction benefits. Pre-transaction benefits are benefits the individual experiences prior to a purchase, such as reduced cognitive effort, ease of use, convenience. Convenience relates to the simplicity and ease of use that could be provided by the payment method. Convenience is an important driver of security based systems use because of its ability to influence times-savings [61]. For example, an individual experiences the benefit of reduced cognitive effort when s/he does not need to remember and type in the correct username/password for each purchase transaction. Indeed, convenience during payment and checkout [61,62] and travel [16] is a driving force for biometrics use.

Post transaction benefits include reduction in fraud, faster transaction speed, and usefulness. For example, an individual experiences reliable authentication knowing that his/her biometric trait is unique and not easily replicated. Usefulness relates to the practicality of the system and whether it allows the user to achieve their tasks effectively [61,63]. Together, the transaction benefits constitute the perceived benefits of the payment methods. Based on these descriptions and the literature showing that convenience and usefulness are major factors in the determination of not only general technology use, but also the use of security systems such as biometrics [32,33,63], this study focuses on perceived usefulness and perceived convenience for perceived benefits.

4. Research model and hypotheses

Our model follows previous experiment based research that demonstrates the effect of stimuli on individual's perceptions and decisions. For example, Xiao and Benbasat [64] examine the effect of different elements of warning messages as independent variables on the individual's perception of bias of product recommendation agents. Wang et al. [65] also examine technology design characteristics (e.g., avatar interfaces) on trust. Prior studies have also assessed the effect of recommendation agent use on user decision outcomes [66]. Hence, we present the research model in Fig. 1, which depicts the three payment authentication methods as the independent variables: (a) biometrics authentication, (b) credit card + PIN authentication, and (c) credit card (token) only authentication. We measure two groups of dependent variables in this study: user perceptions and concerns of payment authentication methods, and outcomes related to the online store. This research model allows us to hypothesize the differential effect of payment authentication methods on users' perceptions - exemplified by security concern, perceived convenience, and perceived usefulness of the payment methods, as well as their belief and behavioral outcomes, which are assessed through trust of online store and willingness to continue using the website account associated with the payment method.

4.1. Comparing the payment authentication methods

Security is an important aspect of electronic payment systems [8]. In this study, we define *security concern* as the degree to which a consumer

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

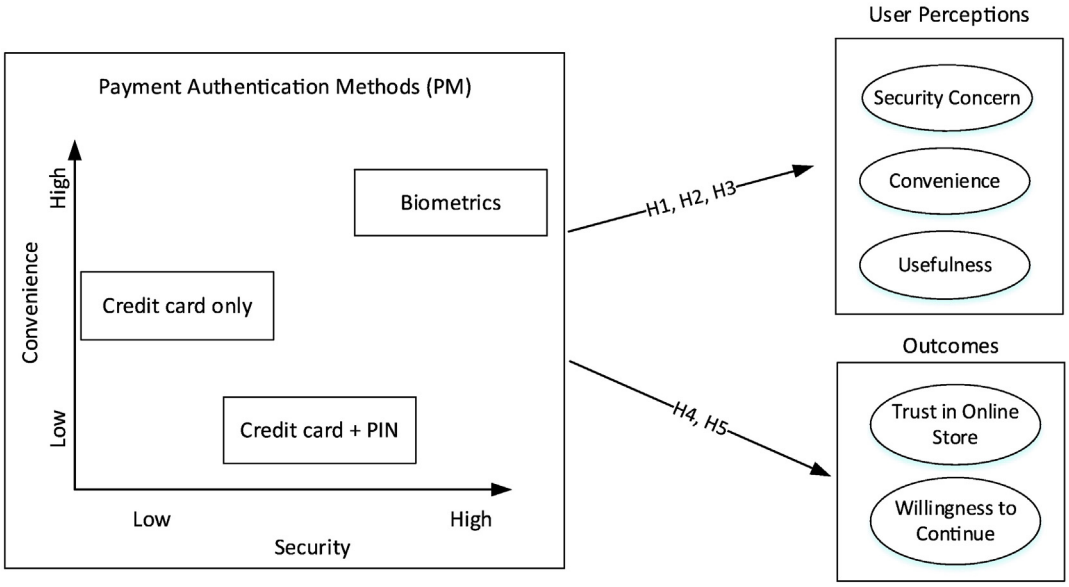

Fig. 1. Research model.

feels unprotected against security threats resulting from the use of the payment method. That is, whether the payment system is safe, secure and can protect the user. While traditional authentication and payment approaches for online transactions such as credit card and credit card + PIN can be replaced when compromised, biometrics data consists of irrevocability. That is, if compromised it becomes impossible to re-issue the individual with a replacement fingerprint [54]. Security breaches involving organizations that are payment cards industry (PCI) compliant, yet lacked proper security safeguards have been known to occur (e.g. Target, Heartland). In such breaches, individuals' card information and personally identifiable information were compromised and stolen. We argue that the effects of biometrics authentication on individuals' security concern are such that it reduces their concern, more so than credit card only or credit card + PIN. Though it has not been empirically validated in IS, biometric authentication in electronic payments has been generally viewed as providing more security and convenience advantages over credit card authentication (e.g. three-digit verification) methods [10,11] and PIN based methods [6]. In fraud reduction, whereas prevailing approaches like password and credit card numbers can be illicitly acquired by direct observation and then repudiated [40], biometrics authentication provides more accurate and reliable user authentication [67]. In addition, given that biometric properties such as fingerprint, iris, and keystroke are unique to each individual, the impersonation of identity is less of a problem [41]. Given these arguments, we hypothesize:

H1: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will perceive less security concern than those using (a) credit card only and (b) credit card + PIN authentication.

Convenience is a relevant factor in online transactions [80] and especially so in the evaluation of authentication methods in an e-commerce context [16,81]. Convenience is the ability to reduce a person's non-monetary costs (i.e., time, energy and effort) when purchasing or using goods and services [80,82–84]. As individuals look for simpler, faster, and easier ways to accomplish tasks, the desire for technologies that help them overcome constraints of time and cognitive loads will increase. Typing in credit card or PIN numbers is no longer required when biometrics authentication linked to a payment method is in place. Hence, it should provide an increased level of convenience. A recent survey notes that about 75% of 16–24 year olds feel comfortable with biometric security, while 69% believe it is easier and faster than using passwords or PINs [68]. The notion is that using biometrics authentication method (e.g., iPhone TouchID) to make a payment eliminates the requirement for personal information entry during the checkout process – and therefore reduces one's susceptibility to direct observation of the information. This not only presents more security, but also more convenience to the user. Even though browser auto-fill features may provide users the convenience of saving their credit cards in browsers, vulnerabilities inherent in browsers (e.g., JavaScript, ActiveX, and Flash) may still present some security concerns. Hence, we hypothesize:

H2: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will perceive more convenience than those using (a) credit card only and (b) credit card + PIN authentication.

Perceived usefulness of payment method is the extent to which a user believes that using the payment method would provide fitness of performing the task and enhance his/her productivity [69]. Usefulness relates to the practicality of the system and whether it allows the user to achieve their tasks effectively [3,4]. Perceived usefulness has been argued to be the only belief that consistently influences user intention in the later stages of IS use [70]. Given that this study assesses the individual's perception after the use the technology, perceived usefulness captures the individual's ex-post evaluation of the payment authentication method. An individual may find it more useful to unlock an iPhone with TouchID (fingerprint biometrics) than punching a four-digit number. Hence, we posit that fingerprint biometrics authentication for payment will be perceived as useful and practical for the task, more so than other traditional payment authentication methods. Hence, we hypothesize:

H3: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will perceive more usefulness than those using (a) credit card only and (b) credit card + PIN authentication.

Even though the focus of this study is more on user perceptions of the payment authentication methods, we also assess the individual's trust of the online store, as well as their willingness to continue using the website account associated with the payment method as outcomes of payment authentication methods. Trust is the belief that the trustee makes an effort to fulfill the trustor's expectations without taking advantage of the consumer [50]. Based on the general concept of trust, we define trust of an online store as the individual's subjective belief that the online store will fulfill its obligations, as the individual

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

Table 2
Factorial design – treatment combinations.

		Level of security		
		Less secure	Secure	More secure
Level of convenience	Less convenient	NC (not considered)	Payment using credit card + PIN	NC
	Convenient	Payment using credit card authentication	NC	NC
	More convenient	NC	NC	Payment using fingerprint authentication

understands them. The online store is the vendor, website, or company from whose store the individual is transacting. Past experiences such as familiarity [23] and behaviors such as product use [65] are recognized as predictors of trust in the literature. Following the literature on the effect of product use on trust, our study seeks to understand the effect of the use of a payment authentication method on the individual's trust of the online store as well as his or her willingness to continue using the website account in the future. In his study of trust of online firms, Bhattacherjee [23] refers to trust as an expectation of future behavior. When an individual is provided an option to make payments in an online store using biometrics authentication, it may create a belief that the store is making an effort to fulfill the individuals' transaction expectations, and therefore may help the individual estimate the likelihood of the online store's future behavior such as revising the online store. Previous studies have used technology artifacts to assess user trust beliefs. For example, Wang, Qiu, Kim and Benbasat [65] examined and found significant, the effects of explanation facilities on cognition-based and affect-based trust.

Willingness to continue using the website account of the online store in the future is another outcome that may result from using secure payment authentication methods that online stores implement on their website [71]. It is conceptualized and measured as the likelihood that customers will continue using the website account that is tied to the payment authentication method for future online shopping. Hence, we hypothesize:

H4: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will express more trust of the online store than those using (a) credit card only and (b) credit card + PIN authentication.

H5: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will be more willing to continue using the website account than those using (a) credit card only and (b) credit card + PIN authentication.

5. Research method

5.1. Research design

In order to empirically validate the research model and to test the proposed hypotheses, we conducted an experiment-based survey. For the experiment, we developed a simple simulated website with three different payment authentication methods (i.e., a credit card authentication, a credit card payment with personal identification number (PIN), and a fingerprint biometric authentication linked to a credit card payment). Considering security and convenience as key factors of the three payment authentication methods, we developed the following treatment for a factorial design of the experiment, depicted on Table 2.

We make an assumption that a credit card only authentication method is considered less secure but more convenient than a credit card + PIN authentication method; a credit card + PIN authentication method is considered less secure than the biometric authentication method and less convenient than credit card only authentication; and a fingerprint-based biometrics authentication method is more convenient and more secure than both credit card only and credit card + PIN authentication methods.

5.2. Experimental procedure

Fig. 2 shows the experiment procedures of the three phases in detail. Before subjects were exposed to the treatments, they went through an orientation that was part of the pre-phase registration process. In the orientation section, the subjects were provided the general procedures of the experiment including creating a user account for the simulated website, creating a mock credit account, logging into the website, and browsing the website.[2] They were not allowed to purchase songs in this stage. After the orientation section, subjects were randomly assigned to opening one of three different payment authentication methods: group 1 for a credit code, group 2 for a credit code + PIN, and group 3 for a fingerprint biometrics authentication linked to a credit code payment. For group 3, they created an account for the mock website and scanned a thumb finger using a fingerprint reader as a part of the registration process. The reader encrypts and stores the individual's biometric information in a database, which would be used later in the purchase/payment process. After they completed the pre-survey, they were asked to login to the website using their ID and password created in the registration process, and to take time browsing and selecting songs to purchase. After they selected songs, they purchased songs using the payment authentication method that was assigned to them in the pre-phase stage.

Like a typical e-commerce transaction using a credit card payment, the subjects of the credit card authentication payment group (i.e., Group 1) provided only their credit code for their payment; it is a control group of the study. For Group 2 (i.e., a credit card payment method with a PIN), they provided their credit code number along with a PIN that requires additional an authentication step. For the biometric payment method group (i.e., Group 3), they made payment by simply scanning their finger on a reader rather than typing their credit code number and PIN. This provided convenience to the group, such that they did not need to carry a credit card, cash or a wallet. Finally, at the end of the experiment, subjects completed a post-survey to provide their experience of purchasing and the payment method. This was followed by a quick debriefing and disclosure step. Although subjects were allowed to take as much time as needed, most subjects spent about 30 min to complete the experiment. Even though participants purchased songs, they did not actually download the songs.

As presented in Fig. 2, the data collection procedure consists of three phases: registration process, login process and purchase/payment process. Students in a large public university in the United States were recruited for this experiment. The subjects voluntarily participated in this study for research purposes, extra course credit and received a $10 reward. Although students do not fully represent the e-commerce population, they were employed for this experiment because the experiment required three phases, which is not controllable with general e-commerce consumers in e-commerce websites. A total of 94 students participated in the study, of which 54.3% are female and 44.7% are male. We randomly assigned almost the same number of subjects to each group: 31, 31, and 32 participants for Group 1, 2 and 3, respectively.

[2] Because IRB disallowed use of word "credit card," we actually asked subjects to create a "credit code" for the mock website.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

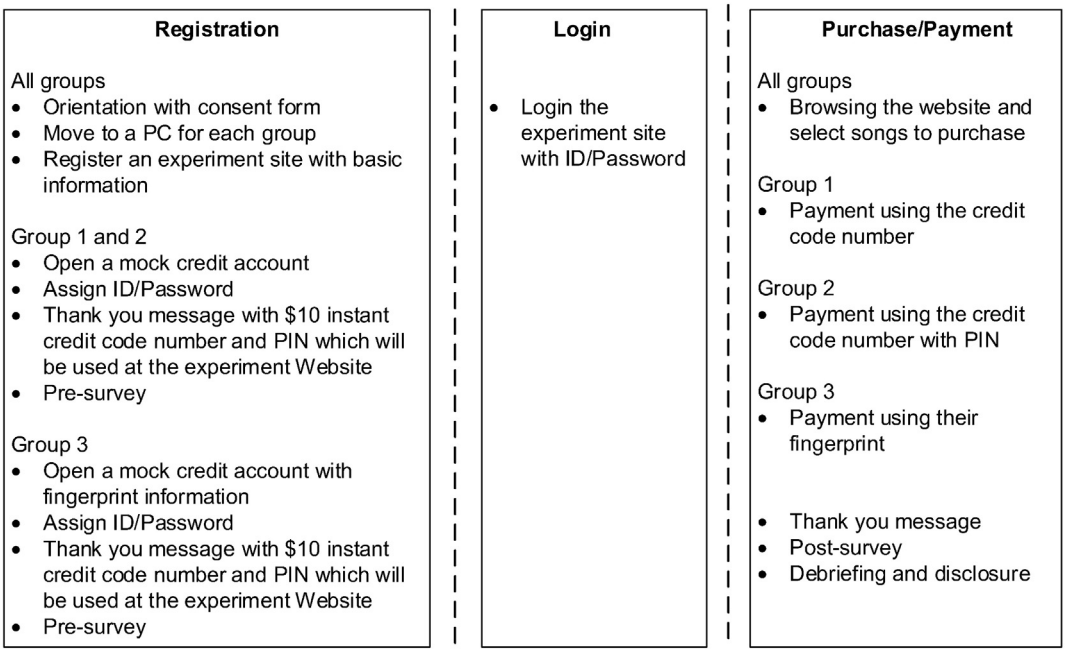

Fig. 2. Experiment process.

5.3. Measurement

Most measurement items were adapted from existing literature; some scales were developed for this study. Appendix B lists the measures used in this study and their sources. The questionnaire accessed the individual's perceptions of each payment method that was randomly assigned to them in terms of usefulness and convenience of the payment authentication methods. Security concern was measured by assessing perceptions of security concerns over the payment methods. For the willingness to continue using the website account associated with the authentication method, we sought to assess whether the individual will use the website account in the future. This measure is slightly distinct from the traditional purchase intention – which seeks to assess the individual's current intent to purchase product/service. The distinction comes with the notion that the individual has already used this account (during the experiment), and we are assessing whether they will use it again in the future.

6. Data analysis and results

6.1. Testing measurement model

ANOVA and independent sample *t*-tests are administered in order to analyze the differences between biometrics authentication for payment and traditional payment authentication methods. IBM SPSS version 24 was used to analyze the data. To investigate the adequacy of the measures, reliability, convergent validity, and discriminant validity of the instruments are examined. Factor loadings of constructs (see Appendix C) show that in general, items load well on their intended factors and lightly on the other factors, thus indicating adequate convergent validity. Table 3 depicts the reliability, correlation, and discriminant validity of constructs.

The measurement testing result shows that all the composite reliabilities are higher than the suggested value of 0.70 and all AVE values are greater than the suggested 0.50, indicating a good convergent validity and measurement model. The diagonal values in Table 3 show the square root of AVEs. Discriminant validity is reached if the value of square root of AVE for each construct is greater than the variance shared between the construct and other constructs in the model [72], and if the items load more strongly on their constructs. Most measurement items show values that are greater than the suggested threshold 0.7 loadings [72,73].

Further, we assess discriminant validity following the recently proposed heterotrait–monotrait ratio (HTMT) method [74]. There are two ways of assessing discriminant validity using the HTMT method. The first way involves comparing and assessing whether the HTMT value is below a threshold. The second way uses a confidence interval to test a null hypothesis of HTMT equal to or more than 1. In the first test, the highest absolute value for our measures was 0.69 (see Table D1 in Appendix D), which satisfies the most conservative threshold of 0.85 [74]. In the second test, all upper confidence intervals are below the value of 1, indicating that all HTMT values are significantly different from 1 (see Table D2 in Appendix D). Therefore, based on these tests, we conclude that discriminant validity of the measurement model is established.

To assess multicollinearity, we examined the variance inflation factor (VIF) statistics. These are suggested to be lower than 3.3 [75]. The VIF values for the constructs are 1.69 (perceived usefulness), 1.36

Table 3
Reliability, correlation, and discriminant validity of constructs (n = 94).

Constructs	Mean (SD)	Alpha	CR	AVE	1	2	3	4	5
1. Usefulness	5.527 (1.245)	0.703	0.871	0.771	0.878				
2. Convenience	6.355 (0.813)	0.730	0.833	0.559	0.461	0.747			
3. Trust	5.220 (1.026)	0.823	0.895	0.740	0.374	0.191	0.860		
4. Security concern	2.560 (1.400)	0.916	0.947	0.857	−0.500	−0.204	−0.602	0.926	
5. Willingness	4.106 (1.514)	0.852	0.908	0.767	0.350	0.342	0.503	−0.467	0.876

Note: SD – standard deviation, CR - composite reliability, AVE - average variances extracted

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

Table 4
Summary F-ratios of ANOVA analysis.

	Sum of squares		Mean square		F-ratio (significance)
	Between groups	Within groups	Between groups	Within groups	
Security concern	30.497	151.772	15.249	1.668	**9.143 (0.000)****
Convenience	1.100	66.563	0.550	0.731	0.752 (0.474)
Usefulness	9.970	134.214	4.985	1.475	**3.380 (0.038)***
Trust	5.459	92.441	2.730	1.016	2.687 (0.073)
Willingness	4.814	208.345	2.407	2.290	1.051 (0.354)

Note: * significant at the 0.05, ** significant at the 0.01 level; bold shows a significant case.

(perceived convenience), 1.81 (security concern), 1.61 (trust). Hence, desired low multicollinearity was observed.

6.1.1. Comparing the payment methods

In order to test the group level differences on the different payment authentication methods, we ran an ANOVA test. The result is summarized in Table 4.

The ANOVA result shows that the F-ratios of security concern and perceived usefulness are significant ($F = 9.143$, $P < 0.001$ and $F = 3.380$, $P < 0.05$, respectively). The result means that there are significant differences between the three different payment methods in terms of security concern and usefulness. Thus, we further ran a set of between-group independent sample *t*-tests to compare the payment authentication methods.

Table 5 shows the results of the *t*-tests. The results show that there are no significant differences between Group 1 (credit card) and Group 2 (credit card + PIN). There are significant differences between Group 1 (credit card) and Group 3 (fingerprint biometrics) in terms of usefulness, trust, and security concern. In addition, there is a significant difference between Group 2 (credit card + PIN) and Group 3 (fingerprint biometrics) in terms of security concern. In other words, this result shows that participants have different degrees of security concerns and the differences are significant across the three different payment methods. In the comparison between Group 1 (credit card) vs. Group 3 (fingerprint), the results show that individuals had more security concern with the credit card method of payment (mean = 3.129) than they did with fingerprint biometrics (mean = 1.792). This difference is statistically significant ($t = -4.161$, P-value < 0.01). Hence, H1a is supported. In the comparison between Group 2 (credit card + PIN) vs. Group 3 (fingerprint), the results also show that individuals had more security concern with the credit card + PIN method (mean = 2.785) more so than they did for the fingerprint biometric method (mean = 1.792). The mean difference between Group 2 and Group 3 is statistically significant ($t = -3.445$, P-value < 0.01). Hence, H1b is supported. In terms of convenience, there is no statistically significant difference between the credit card payment authentication method (mean = 6.153) and the fingerprint biometrics (mean = 6.117). Similarly, there is no significant difference between credit card + PIN (mean = 6.363) and biometrics (mean = 6.117). Hence, H2a/b are not supported. In terms of usefulness, there is a statistically significant difference ($t = 2.554$, P-value < 0.05) between the credit card payment authentication method (mean = 5.145) and the fingerprint biometrics (mean = 5.938). However, there is no significant difference between credit card + PIN (mean = 5.484) and fingerprint biometrics (mean = 5.938). Hence, H3a is supported and H3b is not supported.

Between credit card only (mean = 4.882) and fingerprint biometrics (mean = 5.438), there is a significant ($t = 2.174$, P-value < 0.05) difference in terms of trust of online store. However, there is no significant difference between credit card + PIN (mean = 5.333) and fingerprint biometrics (mean = 5.438). Therefore, H4a is supported and H4b is not supported. In terms of willingness to continue using the website account associated with the authentication method, the results also show that there are no significant differences between credit card only (mean = 3.807) and fingerprint biometrics (mean = 4.354), and between credit card + PIN (mean = 4.151) and fingerprint biometrics (mean = 4.354). Hence, H5a/b are not supported.

7. Discussion

Made popular by smartphones and smartwatches, the rise of biometric authentication for payment has been linked to lower security

Table 5
Results of independent sample (between-group) *t*-test.

Group 1 (credit card) vs. Group 2 (credit card + PIN)						
	Group 1 Mean (SD)	Group 2 Mean (SD)	Mean differences (G2 - G1)	SE	*t*-Statistic	P-value
Security concern	3.129 (1.548)	2.785 (1.324)	−0.344	0.366	−0.940	0.351
Convenience	6.153 (0.848)	6.363 (0.648)	0.210	0.192	1.094	0.279
Usefulness	5.145 (1.367)	5.484 (1.180)	0.339	0.324	.044	.301
Trust	4.882 (1.097)	5.333 (1.000)	0.452	0.267	1.694	0.096
Willingness	3.807 (1.736)	4.151 (1.250)	0.344	0.384	0.896	0.374
Group 1 (credit card) vs. Group 3 (fingerprint)						
	Group 1 Mean (SD)	Group 3 Mean (SD)	Mean differences (G3 - G1)	SE	*t*-Statistic	P-value
Security concern	3.129 (1.548)	1.792 (0.938)	−1.337	0.321	−4.161	**0.000****
Convenience	6.153 (0.848)	6.117 (1.022)	−0.036	0.237	−0.152	0.880
Usefulness	5.145 (1.367)	5.938 (1.083)	0.792	0.310	2.554	**0.013***
Trust	4.882 (1.097)	5.438 (0.921)	0.556	0.256	2.174	**0.034***
Willingness	3.807 (1.736)	4.354 (1.514)	0.548	0.410	1.336	0.187
Group 2 (credit card + PIN) vs. Group 3 (fingerprint)						
	Group 2 Mean (SD)	Group 3 Mean (SD)	Mean differences (G3 - G2)	SE	*t*-Statistic	P-value
Security concern	2.785 (1.324)	1.792 (0.938)	−0.993	0.288	−3.445	**0.001****
Convenience	6.363 (0.648)	6.117 (1.022)	−0.246	0.216	−1.135	0.261
Usefulness	5.484 (1.180)	5.938 (1.083)	0.454	0.285	1.591	0.117
Trust	5.333 (1.000)	5.438 (0.921)	0.104	0.242	0.430	0.669
Willingness	4.151 (1.250)	4.354 (1.514)	0.203	0.350	0.581	0.563

Note: SD – standard deviation, SE – standard error, * significant at the 0.05 and ** significant at the 0.01 level, bold shows a significant case.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

Table 6
Summary of hypotheses testing results.

Hypothesis	Result
H1: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will perceive less security concern than those using (a) credit card only and (b) credit card + PIN authentication.	S**/S**
H2: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will perceive more convenience than those using (a) credit card only and (b) credit card + PIN authentication.	NS/NS
H3: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will perceive more usefulness than those using (a) credit card only and (b) credit card + PIN authentication	S**/NS
H4: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will express more trust in the online store than those using (a) credit card only and (b) credit card + PIN authentication.	S**/NS
H5: Comparing biometrics authentication with other payment authentication methods, individuals using biometrics authentication will be more willing to continue using the website account than individuals using (a) credit card only and (b) credit card + PIN authentication.	NS/NS

Note: S: supported, NS: not supported, * significant at the 0.05 level, ** significant at the 0.01 level.

concerns (e.g. preventing identity theft), and increased convenience [13]. Hence, biometric authentication based payment has taken a center stage position in the e-commerce and m-commerce electronic payment arena, deserving research to examine how they are perceived in comparison to traditional payment authentication systems. Using a set of data collected from an experiment-based survey, we use ANOVA and *t*-tests to analyze the difference in perceptions between biometrics authentication based payment and traditional payment authentication methods. Table 6 summarizes the results of the hypotheses testing.

We find that individuals perceive fingerprint biometrics with less security concern than credit card only or credit card + PIN payment authentication methods. This supports biometrics literature that suggests that biometrics is more secure [10]. Going by the increased number of the U.S. consumers affected by identity theft and credit card fraud [76,77], this suggests that individuals that fall victim to these types of crimes may constitute a large number of the users of biometric authentication. These consumers may represent a growing market segment. Hence, there is a need for practitioners to identify and target marketing to this segment, and for more research to investigate how prior identity theft experience affects e-commerce and m-commerce transaction behavior.

In addition, we find that individuals who are less concerned with the security of biometrics authentication method may also find biometrics authentication method more useful. These results are useful in the design of electronic payment systems, in creating value for consumers, and for addressing security concerns in payment systems. Our findings show that consumers with less security concern of biometrics authentication method also trust the online store. This means that consumers tend to trust organizations that make the effort to provide security protective technologies (e.g. biometrics). Indeed, Ponemon [16] notes that 65% of German and 46% of US consumers surveyed, do not trust online firms that rely only on usernames and passwords for authentication. In other words, consumers tend to trust online firms and websites that provide stronger authentication procedures.

Contrary to our expectation, the results do not support that willingness to continue using the website account associated with biometrics authentication method is significantly different from those associated with credit card or credit card + PIN methods. Our interpretation is that using a biometrics authentication payment method that is tied to website account may not be the only reason that users are willing to continue using the website account. For instance, an individual could create a website account at an e-commerce website such as Amazon.com. This account could be associated with a payment authentication method such as biometrics or credit card + PIN. In this case, the payment authentication method (biometrics or credit card + PIN) serves as one of the security/authentication features offered by the website. However, this feature may not be the main reason users are willing to continue using the website account. There could be other reasons that drive their willingness to continue using that website account in the future.

7.1. Research and practical implications

There are research implications of this study. First, the study brought together biometrics authentication for electronic payment, and empirically compared it with traditional electronic payment authentication methods. Our study empirically corroborates previous non-empirical suggestions about security perceptions people have about biometrics authentication based payment in comparison with other authentication methods [10,11,68]. This is a context that is becoming more important as e-commerce, m-commerce, and mobile payments through biometrics continue to grow. This context provided an evidence for the importance of the individual's perceptions, concerns, and beliefs in the use of biometrics authentication for electronic payments. Our study is the first to empirically evaluate payment authentication methods in IS research. By explicating the context of biometrics authentication based payment in IS research, this study contextualized the valence framework. According to Whetten [26], sensitivity to contexts is important, it helps us derive meaning, as well as discuss the limits of generalizability. Given that authentication for payment is a crucial part of e-commerce transaction, and that there is a dearth of research that incorporates authentication and payment methods, the implication of this study is unique in its examination of the perceptions and outcomes of electronic payment authentication methods in an e-commerce context.

Second, mainly focusing on security, convenience, and usefulness aspects of the payment authentication methods, we contribute to the validation of the valence framework. Specifically, an implication of this research is in testing out and providing insight into the individuals' assessment of risks and benefits in the evaluation of security technology usage. We proposed and tested the hypotheses that individuals would evaluate the positive (convenience and usefulness) and negative (security concern) aspects of the valence framework. There is evidence of the valence evaluation, which is revealed in the support we found in the evaluation of a positive (usefulness) and a negative (security concern) valence. Hence, validate the valence framework as the evaluation of both positive and negative feelings toward a payment authentication method.

Lastly, though previous studies have researched payment methods in ecommerce, we go a step further in explicating the security aspects of payment methods through their authentication. Hence, we shift the focus from a broad view of payment methods to the specifics of their authentication/security aspects. By doing so, we address a core security functionality that supports successful electronic payments in e-commerce. This core functionality is authentication (being able to verify and validate that individuals are who they say they are). Using three different payment authentication methods, we access their effects on individuals' perceptions, beliefs, and behavioral outcomes. Furthermore, we separate the dependent variables into two groups. The first group is perceptions and concerns related to the payment authentication methods. The second group is outcomes related to the online store. By doing so, we delineate and capture both (1) the user's perceptions of the payment authentication methods, and (2) the effect of use on the individual's trust of the online store and willingness to continue using the website account.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

In terms of practical implication, our findings suggest insights. First, in demonstrating the significant differences when comparing biometrics authentication with traditional authentication methods, this research validates this largely observed but empirically untested notion of biometrics authentications. Among the three payment authentication methods, individuals expressed the least security concern in biometrics authentication payment method. This result confirms the biometrics technical reports that have suggested that because token based systems such as credit cards and knowledge based systems such as PINs cannot differentiate between authorized and unauthorized users, they are less able to provide security protections required for e-commerce transactions [30,40]. Given that our results suggest that individuals deem biometrics more secure than the other payment authentication methods, practitioners are encouraged to pursue the integration of biometrics authentication options in their e-commerce and m-commerce payment methods.

Even though we did not find a statistically significant difference between credit card and credit card + PIN, their mean differences suggest that individuals expressed more security concern for the credit card payment authentication method than they did for credit card + PIN. This may indicate that the use of payment methods that utilize multi-factor authentication is seen as more secure than others. Amid the clamor around credit card fraud, identity theft [76], and financial data breaches, this result is further indication that practitioners in e-commerce should seek to include authentication and payment options that not only provide improved security, but provide multi-factor authentication. This may give online consumers a perception of increased security protection. Indeed, the authentication method used by Equifax that resulted in the breach of 143 million customers has been described as an "outdated and insufficient consumer authentication method" ([78], p. 1). As a result, experts suggest that at the least, consumers should be provided with two-factor authentication method. In addition, biometrics authentication should be provided to further bolster security [79].

As described earlier, through the study's context – biometrics versus traditional authentication – evidence is provided for the importance of the individual's perceptions, concerns, and beliefs in using biometrics authentication for electronic payments. A major goal for practitioners in advertising and marketing is to influence individuals' perceptions concerning their products. Having shown that there are indeed significant differences in how individuals view the different payment authentication methods in terms of security, usefulness, and trust; this serves as an empirical validation that could be referenced to support and justify the deployment of biometrics authentication in e-commerce.

Second, individuals that used biometrics authentication expressed trust of online store more so than those that used credit card only or credit card + PIN. This means that consumers tend to trust online firms that provide authentication methods with stronger security. Trust is important in helping practitioners create value for customers and for developing competitive advantages. This result suggests that e-commerce sites should continue to consider strong requirements for security in the payment method options provided to online consumers, in order to create and maintain trust. In addition, the technologies that are provided for the authentication of payment methods should allay consumer concerns for security. An e-commerce site and its product choices may be appealing to individuals, but if the authentication and payment methods available to the user are lacking in terms of security, it may reduce the likelihood that consumers will complete transactions on the e-commerce site. Considering today's cybercrime climate, this research may serve to encourage practitioners to seek more secure authentication based payment methods such as biometrics and other multi-factor authentication systems. By comparing three payment authentication methods, this study paves the way for practitioners to understand how integrating biometrics authentication for payment could positively affect their relationships with consumers.

7.2. Limitations and future directions

This research is the first at comparing and understanding how individuals perceive payment authentication methods for e-commerce payment in IS research. Thus, meaning that it is not yet fully understood or established, and may require more research in order to increase our understanding of how the use of biometrics authentication for payment influences willingness to continue use. It should be noted that prior technology use is only one of the several possible reasons for individuals to continue use. The continuance literature suggests that satisfaction is a key factor in technology use continuance [26]. Hence, an opportunity for future research is to include constructs such as satisfaction and enjoyment in the model. In addition, manipulating specific characteristics of each payment authentication method may increase perceptions and willingness to continue use. This study used an experiment methodology to collect data and then analyzed the data using ANOVA and *t*-tests, which are traditional analysis methods for experiment data. In addition to these types of analyses, future research could also perform structural path modeling and multi-group analysis in order to understand the strengths of relationship between the constructs of interest, as well as understand the most powerful drivers of willingness to continue use.

Common with experiments is the limitation of external validity. Since individuals are not actually expending their income on the purchase, the influence of the authentication methods on security concerns may be reduced. Future research could include mental conditions that seek to place some of the responsibility on the participants of the experiment in order to ensure that participants are placed in situations close to reality. Another limitation is that although we collected data through experiments using a mock website for the manipulation of different methods of payment, the data is about consumers' perception of a single mock e-commerce site. Thus, future research can employ several different e-commerce sites to improve the validity of results. As security breaches increase, future studies can also investigate how identity theft experience directly influences e-commerce transactions and moderates the relationship between security concerns and e-commerce transactions.

Security concern was conceptualized and operationalized at a general level. Although the conceptualization provided adequate perceptions of security concerns, future research could develop and evaluate dimensions of security (e.g., storage, access) to understand how perceptions differ based on specific dimensions. Furthermore, another limitation in this study is the accounting for social desirability bias. While we used willingness measures (e.g., "I would be willing to continue using …" versus "I intend to use…") that are less affected by social desirability [80], future research should design a data collection strategy that reduces this bias.

Lastly, it is possible that other variables of interest such as privacy concern would provide more insights to individuals' perceptions of biometrics in comparison to other payment authentication methods. The possibility that an individual's biometrics information could be lost, breached, or used for purposes other than its original intent raises a concern. Therefore, evaluating privacy concern in terms of the data collection, secondary use, errors, and unauthorized access [81] could be useful for future research. Like other advanced technology (e.g. location-based services), biometrics technology is double-edged, providing both positive and negative aspects. On the one side, individuals benefit from reduced cognitive effort and increased security, while on the other, giving up a level of privacy. An in-depth understanding of individuals' perception over the privacy of their biometrics data is important, not only because it has implications for the effectiveness of identification and authentication in information systems, but also because of its impact on standards and guidelines in dealing with security and privacy protection of biometrics data collection and storage. As biometric authentication technology expands more into m-commerce, social media and the cloud, it becomes even more important to gain more understanding of individuals' perception of biometrics authentication.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

Appendix A. Studies on biometrics adoption and payment method adoption

Study source	Theory	Payment/biometrics	Variables	Findings
Biometrics adoption studies				
James, Pirim, Boswell, Reithel and Barkhi [32] Uses retina to explain and predict the adoption of biometrics.	TAM	Biometrics	Perceived ease of use, perceived usefulness, perceived security, perceived need for privacy, perceived physical invasiveness, situational characteristics, intention to use	With an R-squared of 59%, ease of use, usefulness and invasiveness have significant direct effects on intention.
Ngugi, Kamis and Tremaine [36] Uses typing patterns to explain and predict biometrics adoption	TAM	Biometrics	Perceived system security, perceived false rejection rate, perceived false acceptance rate, perceived system invasiveness, biometric system trust, facilitating conditions, intention to use	With an R-squared of 55.3%, facilitating conditions, biometric system trust and perceived system invasions were significant in their effect on intention to use.
Byun and Byun [31] Uses fingerprint to explain and predict biometrics adoption	None	Biometrics	Perceived risks, perceived benefits, personal innovativeness, consumer value, intention to adopt.	Perceived benefits and perceived risks have significant direct effect on consumer value. Consumer value (the only direct link to intention) has a significant effect on intention to adopt
Soh, Wongand and Chan [34] Predicts biometrics adoption in online applications	TAM	Biometrics	Perceived ease of use, perceived usefulness, perceived risk, perceived credibility, personal innovativeness, computer self-efficacy, usage experience, intention to use	With an R-squared of 60.9%, Perceived ease of use, perceived risk, perceived credibility, personal innovativeness and computer self-efficacy have significant direct effects on intention.
Lancelot Miltgen, Popovič and Oliveira [33] Uses iris scanning technology to explain and predict biometrics adoption	TAM, UTAUT, DOI	Biometrics	Compatibility, perceived usefulness, perceived ease of use, social influence, facilitating conditions, perceived risks, concern for data privacy, trust in technology, innovativeness, intention to accept technology, intention to recommend the technology	With an R-squared of 42%, perceived usefulness, perceived risks, trust in technology, and innovativeness have significant direct effects on intention. Perceived ease of use and social influence were not significant.
Morosan [37] Examines travelers' adoption of traveler specific biometric technology	TAM	Biometrics	Perceived usefulness, perceived ease of use, perceived security, perceived privacy, perceived innovativeness, attitudes, intentions	With an R-squared of 77%, attitudes have a positive and significant effect on intentions
Wells, Campbell, Valacich and Featherman [35] Examines the general adoption biometrics application	TAM	Biometrics	Personal innovativeness, novelty, attitude, overall reward, overall risk, behavioral intention	With an R-squared of 42%, attitude has a significant effect on intention. Novelty, perceived risk and perceived reward has significant effect on attitude. Personal innovativeness has a significant effect
Payment methods studies				
Kim, Tao, Shin and Kim [90]	None	Payment	Technical protections, transaction procedures, security statements, e-payment objective dimension, perceived security in EPS, Perceived Trust in EPS, e-Payment Subjective Dimension, Perceived Security in EPS, Perceived Trust in EPS, EPS Use	Technical protections and Security statements have significant effects on perceived security in EPS Transaction procedures and Technical protections have significant effects on perceived trust in EPS. Perceived security in EPS has significant on perceived trust in EPS. Perceived security in EPS and Perceived trust in EPS are also significant on EPS use
Lu, Yang, Chau and Cao [91] Mobile Payment based on valence and trust framework	Trust transfer	Payment	Perceived cost, perceived risk, relative advantage, compatibility, image, internet payment trust, initial mobile payment trust, intention	With an R-squared of 44.2%, perceived cost, perceived risk, relative advantage, compatibility, image, initial mobile payment trust has significant direct effects on intention
Zhang and Li [27] An evaluation of determinants of payment method choices offered by sellers in online auctions	None	Payment	Price of product, used product, warranted product, negative reputation rating, volume of transactions, selling experience, buying experience,	Using a profit analysis, the results shows that product attributes have strong effect on payment method choice that sellers provide. Volume of sales affect the payment method choices while negative ratings reduce the probability of offering credit cards payment options

Note: IDT - Information diffusion theory; TAM –Technology Acceptance Model; DOI – Diffusion of Innovations

Appendix B. Measurement items for constructs

Constructs	Measurement items	Source
Security concern of payment method	While shopping at this online store, I felt that the payment method was:	
	PS1: 1- Unsafe/7 – safe (R)	[50]
	PS2: 1- Not secure/7 – secure (R)	[88]
	PS3: 1 Protected/7 – unprotected	[88]
Convenience of payment method	While shopping at this online store, I felt that the payment method was:	
	CON1: 1- Difficult/7 – easy	[69,82,83]
	CON2: 1- Inconvenient/7 – convenient	[84]
	CON3: 1- Simple/7 – complex (R) (dropped)	New
	CON4: 1- Time-consuming/7- fast	New
Usefulness of payment method	While shopping at this online store, I felt that the payment method was:	
	USE1: 1- Inexpensive/7 – expensive (R) (dropped)	[69]

(continued on next page)

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

(*continued*)

Constructs	Measurement items	Source
	USE2: 1- Useful/7 – not useful (R)	[69]
	USE3: 1- Practical/7 – impractical (R)	New
Trust of online store	TRU1: This online store is trustworthy.	[50,85]
	TRU2: This online store is reliable.	[86]
	TRU3: General trust in this online store	[87]
Willingness to continue using the website account	WIL1: be willing to continue using this account in the future for online shopping.	[85]
	WIL2: be willing to continue using this account for general shopping	[89]
	WIL3: will continue buying songs from this online store	[71]

Note: scales of measurement items not mentioned in the table were anchored with end points with strongly disagree (1) and strongly agree (7).

Appendix C. Factor loadings

	Convenience	Willingness	Security Concern	Trust	Usefulness
PS1	−0.240	−0.489	**0.964**	−0.572	−0.473
PS2	−0.199	−0.475	**0.971**	−0.570	−0.469
PS3	−0.099	−0.305	**0.834**	−0.548	−0.345
CON1	**0.842**	0.282	−0.066	0.111	0.284
CON2	**0.780**	0.258	−0.109	0.051	0.339
CON4	**0.735**	0.251	−0.135	0.204	0.256
USE2	0.414	0.288	−0.385	0.343	**0.872**
USE3	0.396	0.325	−0.489	0.315	**0.884**
TRU1	0.184	0.501	−0.589	**0.870**	0.308
TRU2	0.158	0.432	−0.530	**0.904**	0.279
TRU3	0.148	0.355	−0.416	**0.799**	0.293
WIL1	0.338	**0.921**	−0.532	0.519	0.382
WIL2	0.318	**0.887**	−0.381	0.463	0.244
WIL3	0.224	**0.817**	−0.260	0.307	0.213

Note: bold shows factor loadings of their intended factors.

Appendix D. Heterotrait-monotrait (HTMT) [74]

Table D1
Heterotrait-monotrait ratio of the correlations (HTMT).

	Convenience	Willingness	Security concern	Trust
Willingness	0.391			
Security concern	0.144	0.490		
Trust	0.191	0.574	0.690	
Usefulness	0.477	0.430	0.613	0.493

Table D2
Confidence intervals of HTMT.

	Original sample (O)	Sample mean (M)	Confidence intervals	
			2.50%	97.50%
Willingness - convenience	0.391	0.403	0.174	0.668
Security concern - convenience	0.144	0.209	0.073	0.442
Security concern - willingness	0.490	0.489	0.300	0.663
Trust - convenience	0.191	0.250	0.096	0.462
Trust - willingness	0.574	0.571	0.403	0.718
Trust - security concern	0.690	0.690	0.554	0.807
Usefulness - convenience	0.477	0.474	0.233	0.740
Usefulness - willingness	0.430	0.436	0.204	0.702
Usefulness - security concern	0.613	0.629	0.414	0.833
Usefulness - trust	0.493	0.509	0.275	0.754

References

[1] NACHA, ACH volume grows to more than 25 billion payments and $43 trillion in value in 2016, https://www.nacha.org/news/ach-volume-grows-more-25-billion-payments-and-43-trillion-value-2016 2017, Accessed date: 1 June 2017.

[2] G. Torkzadeh, G. Dhillon, Measuring factors that influence the success of internet commerce, Inf. Syst. Res. 13 (2002) 187–204.

[3] Y.A. Au, R.J. Kauffman, Should we wait? Network externalities, compatibility, and electronic billing adoption, J. Manag. Inf. Syst. 18 (2001) 47–63.

[4] R. Bapna, P. Goes, K.K. Wei, Z. Zhang, A finite mixture logit model to segment and predict electronic payments system adoption, Inf. Syst. Res. 22 (2011) 118–133.

[5] D. Abrazhevich, Electronic Payment Systems: A User-Centered Perspective and Interaction Design, Technische Universiteit Eindhoven, Eindhoven, The Netherlands, 2004.

[6] F. Fintech, Fintech experts say mobile and biometric authentication to replace PINs within five years, http://www.fintech.finance/01-news/fintech-experts-say-mobile-and-biometric-authentication-to-replace-pins-within-five-years/ 2017, Accessed date: 1 June 2017.

[7] R. Kalakota, A.B. Whinston, Electronic commerce: a manager's guide, Addison-Wesley Professional, 1997.

[8] C.M. Kahn, J.M. Liñares-Zegarra, Identity theft and consumer payment choice: does security really matter? J. Financ. Serv. Res. (2015) 1–39.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

[9] T. Sharp, A. Shreve-Neiger, W. Fremouw, J. Kane, S. Hutton, Exploring the psychological and somatic impact of identity theft, J. Forensic Sci. 49 (2004) 131–136.
[10] R. Clodfelter, Biometric technology in retailing: will consumers accept fingerprint authentication? J. Retail. Consum. Serv. 17 (2010) 181–188.
[11] V.F. Kleist, Building technologically based online trust: can the biometrics industry deliver the online trust silver bullet? Inf. Syst. Manag. 24 (2007) 319–329.
[12] A. Hovav, R. Berger, Tutorial: identity management systems and secured access control, Commun. Assoc. Inf. Syst. 25 (2009) 42.
[13] T.G. Zimmerman, G.F. Russell, A. Heilper, B.A. Smith, J. Hu, D. Markman, J.E. Graham, C. Drews, Retail Applications of Signature Verification, Defense and Security, International Society for Optics and Photonics, 2004 206–214.
[14] Q. Tao, R. Veldhuis, Biometric authentication system on mobile personal devices, IEEE Trans. Instrum. Meas. 59 (2010) 763–773.
[15] Juniper, Biometric Authentication App Downloads to Reach 770 Million by 2019, Juniper Research, 2015.
[16] Ponemon, Moving Beyond Passwords: Consumer Attitudes on Online Authentication, 2013.
[17] D. Kumar, R. Yeonseung, K. Dongseop, A survey on biometric fingerprints: the cardless payment system, Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on 2008, pp. 1–6.
[18] T.G. Zimmerman, G.F. Russell, A. Heilper, B.A. Smith, J. Hu, D. Markman, J.E. Graham, C. Drews, Retail applications of signature verification, Defense and Security, International Society for Optics and Photonics 2004, pp. 206–214.
[19] Accenture, Biometrics and privacy: a positive match, Accenture, 2012.
[20] J. Lee, Report shows growing public acceptance of biometric authentication. BiometricUpdate, http://www.biometricupdate.com/201507/report-shows-growing-public-acceptance-of-biometric-authentication 2015, Accessed date: 6 June 2017.
[21] M. Zviran, W.J. Haga, Password security: an empirical study, J. Manag. Inf. Syst. 15 (1999) 161–185.
[22] D. Gefen, P.A. Pavlou, The boundaries of trust and risk: the quadratic moderating role of institutional structures, Inf. Syst. Res. 23 (2012) 940–959.
[23] A. Bhattacherjee, Individual trust in online firms: scale development and initial test, J. Manag. Inf. Syst. 19 (2002) 211–241.
[24] D.J. Kim, A study of the multilevel and dynamic nature of trust in E-commerce from a cross-stage perspective, Int. J. Electron. Commer. 19 (2014) 11–64.
[25] S. Sarker, J.S. Valacich, An alternative to methodological individualism: a non-reductionist approach to studying technology adoption by groups, MIS Q. 34 (2010) 779–808.
[26] D.A. Whetten, What constitutes a theoretical contribution? Acad. Manag. Rev. 14 (1989) 490–495.
[27] H. Zhang, H. Li, Factors affecting payment choices in online auctions: a study of eBay traders, Decis. Support. Syst. 42 (2006) 1076–1088.
[28] K.A. Carow, M.E. Staten, Debit, credit, or cash: survey evidence on gasoline purchases, J. Econ. Bus. 51 (1999) 409–421.
[29] K. Havenetidis, Encryption and biometrics: context, methodologies and perspectives of biological data, Am. J. Appl. Math Stat. 3 (2013) 141–161.
[30] A. Jain, L. Hong, S. Pankanti, Biometric identification, Commun. ACM 43 (2000) 90–98.
[31] S. Byun, S.-E. Byun, Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters, Behav. Inform. Technol. 32 (2013) 217–230.
[32] T. James, T. Pirim, K. Boswell, B. Reithel, R. Barkhi, Determining the intention to use biometric devices: an application and extension of the technology acceptance model, J. Org. End User Comput. 18 (2006) 1–24.
[33] C. Lancelot Miltgen, A. Popovič, T. Oliveira, Determinants of end-user acceptance of biometrics: integrating the "Big 3" of technology acceptance with privacy context, Decis. Support. Syst. 56 (2013) 103–114.
[34] K.L. Soh, W. Wongand, K.L. Chan, Adoption of biometric Technology in Online Applications, Int. J. Bus. Manage. Sci. 3 (2010) 121–146.
[35] J.D. Wells, D.E. Campbell, J.S. Valacich, M. Featherman, The effect of perceived novelty on the adoption of information technology innovations: a risk/reward perspective, Decis. Sci. 41 (2010) 813–843.
[36] B. Ngugi, A. Kamis, M. Tremaine, Intention to use biometric systems, e-Service J. 7 (2011) 20–46.
[37] C. Morosan, Voluntary steps toward air travel security an examination of travelers' attitudes and intentions to use biometric systems, J. Travel Res. 51 (2012) 436–450.
[38] H.-J. Kim, Biometrics, is it a viable proposition for identity authentication and access control? Comput. Secur. 14 (1995) 205–214.
[39] V. Matyáš, Z. Říha, Biometric authentication — security and usability, in: B. Jerman-Blažič, T. Klobučar (Eds.), Advanced Communications and Multimedia Security, Springer, US 2002, pp. 227–239.
[40] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40 (2001) 614–634.
[41] S.S. Hwang, H.J. Lee, S. Cho, Account-sharing detection through keystroke dynamics analysis, Int. J. Electron. Commer. 14 (2009) 109–125.
[42] R.R. Vangala, S. Sasi, Biometric authentication for e-commerce transaction, Imaging Systems and Techniques, 2004, 2004 IEEE International Workshop on (IST) 2004, pp. 113–116.
[43] B. Schneier, The uses and abuses of biometrics, Association for Computing Machinery, Commun. ACM 42 (1999) 136.
[44] A. Chandra, T. Calderon, Challenges and constraints to the diffusion of biometrics in information systems, Commun. ACM 48 (2005) 101–106.
[45] J. Breebaart, B. Yang, I. Buhan-Dulman, C. Busch, Biometric template protection, DuD 33 (2009) 299–304.
[46] E. Kohlwey, A. Sussman, J. Trost, A. Maurer, Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next Generation Biometric Systems, 2011 IEEE World Congress on Services IEEE, Washington, DC, 2011 597–601.
[47] M. Cohn, Biometrics: key to securing consumer trust, Biometric Technol. Today 15 (2007) 8–9.
[48] D.S. Anderson, What trust is in these times-examining the foundation of online trust, Emory LJ 54 (2005) 1441.
[49] P. Rizzo, Capital one survey finds blockchain interest growing at Money20/20, https://www.coindesk.com/capital-one-blockchain-impact-financial-services/ 2015, Accessed date: 11 October 2017.
[50] D. Gefen, E-commerce: the role of familiarity and trust, Omega 28 (2000) 725–737.
[51] P.A. Pavlou, D. Gefen, Building effective online marketplaces with institution-based trust, Inf. Syst. Res. 15 (2004) 37–59.
[52] P.A. Pavlou, D. Gefen, Psychological contract violation in online marketplaces: antecedents, consequences, and moderating role, Inf. Syst. Res. 16 (2005) 372–399.
[53] K. Siau, Z. Shen, Building customer trust in mobile commerce, Commun. ACM 46 (2003) 91–94.
[54] E.A. Whitley, U. Gal, A. Kjaergaard, Who do you think you are? a review of the complex interplay between information systems, identification and identity, Eur. J. Inf. Syst. 23 (2014) 17–35.
[55] J.P. Peter, L.X. Tarpey Sr, A comparative analysis of three consumer decision strategies, J. Consum. Res. (1975) 29–37.
[56] D.J. Kim, D.L. Ferrin, H.R. Rao, Trust and satisfaction, two stepping stones for successful e-commerce relationships: a longitudinal exploration, Inf. Syst. Res. 20 (2009) 237–257.
[57] M.S. Featherman, P.A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective, Int. J. Hum. Comput. Stud. 59 (2003) 451–474.
[58] J.P. Peter, M.J. Ryan, An investigation of perceived risk at the brand level, J. Mark. Res. (1976) 184–188.
[59] S. Glover, I. Benbasat, A comprehensive model of perceived risk of e-commerce transactions, Int. J. Electron. Commer. 15 (2010) 47–78.
[60] R.K. Chellappa, P.A. Pavlou, Perceived information security, financial liability and consumer trust in electronic commerce transactions, Logist. Inf. Manag. 15 (2002) 358–368.
[61] P. Jones, P. Williams, D. Hillier, D. Comfort, Biometrics in retailing, Int. J. Retail Distrib. Manag. 35 (2007) 217–222.
[62] IBIA, Identity Matters, International Biometrics and Identity Association, ibia.org 2016.
[63] D.K. Smetters, R.E. Grinter, Moving from the design of usable security technologies to the design of useful secure applicationsProceedings of the 2002 workshop on New security paradigms, ACM 2002, pp. 82–89.
[64] B. Xiao, I. Benbasat, Designing warning messages for detecting biased online product recommendations: an empirical investigation, Inf. Syst. Res. 26 (2015) 793–811.
[65] W. Wang, L. Qiu, D. Kim, I. Benbasat, Effects of rational and social appeals of online recommendation agents on cognition-and affect-based trust, Decis. Support. Syst. 86 (2016) 48–60.
[66] B. Xiao, I. Benbasat, E-commerce product recommendation agents: use, characteristics, and impact, MIS Q. 31 (2007) 137–209.
[67] A.K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information security, IEEE Trans. Inf. Forensics Secur. 1 (2006) 125–143.
[68] VISA, Generation Z Ready for Biometric Security to Replace Passwords, https://www.visaeurope.com/newsroom/news/generation-z-ready-for-biometric-security-to-replace-passwords 2016, Accessed date: 19 December 2016.
[69] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Q. (1989) 319–340.
[70] A. Bhattacherjee, Understanding information systems continuance: an expectation-confirmation model, MIS Q. (2001) 351–370.
[71] V. Venkatesh, M.G. Morris, B.D. Gordon, F.D. Davis, User acceptance of information technology: toward a unified view, MIS Q. 27 (2003) 425–478.
[72] W.W. Chin, Commentary: issues and opinion on structural equation modeling, MIS Q. 22 (1998) vii–xvi.
[73] J.F. Hair Jr., G.T.M. Hult, C. Ringle, M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), Sage Publications, 2013.
[74] J. Henseler, C.M. Ringle, M. Sarstedt, A new criterion for assessing discriminant validity in variance-based structural equation modeling, J. Acad. Mark. Sci. 43 (2015) 115–135.
[75] A. Diamantopoulos, The error term in formative measurement models: interpretation and modeling implications, J. Modell. Manage. 1 (2006) 7–17.
[76] FTC, Identity theft tops FTC's consumer complaint categories again in 2014, https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014 2015, Accessed date: 14 March 2016.
[77] Javelin, 2016 Identity fraud: fraud hits an inflection point, https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point 2016, Accessed date: 22 March 2016.
[78] KrebsOnSecurity, Fraudsters exploited lax security at Equifax's TALX payroll division, https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/ 2017, Accessed date: 31 October 2017.
[79] J. Blyskal, How to lock down your money after the Equifax breach, https://www.consumerreports.org/equifax/how-to-lock-down-your-money-after-the-equifax-breach/ 2017 Accessed 31 2017.
[80] L. Beck, I. Ajzen, Predicting dishonest actions using the theory of planned behavior, J. Res. Pers. 25 (1991) 285–301.
[81] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. (1996) 167–196.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003

[82] W.J. Doll, G. Torkzadeh, The measurement of end-user computing satisfaction, MIS Q. 12 (1988) 259–274.
[83] G.C. Moore, I. Benbasat, Development of an instrument to measure the perceptions of adopting an information technology innovation, Inf. Syst. Res. 2 (1991) 192–222.
[84] V. Swaminathan, E. Lepkowska-White, B.P. Rao, Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange, J. Comput.-Mediat. Commun. 5 (1999).
[85] S.L. Jarvenpaa, N. Tractinsky, M. Vitale, Consumer trust in an internet store, Inf. Technol. Manag. 1 (2000) 45–71.
[86] D. Larcker, L. Parker, Perceived usefulness of information: a psychometric examination, Decis. Sci. 11 (1980) 121–134.
[87] R.C. Mayer, J.H. Davis, The effect of the performance appraisal system on trust for management: a field quasi-experiment, J. Appl. Psychol. 84 (1999) 123.
[88] M.K. Cheung, M.K.O. Lee, Trust in internet shopping: instrument development and validation through classical and modern approaches, J. Glob. Inf. Manag. 9 (2001) 23–35.
[89] K. Mathieson, Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior, Inf. Syst. Res. 2 (1991) 173–191.
[90] C. Kim, W. Tao, N. Shin, K.-S. Kim, An empirical study of customers' perceptions of security and trust in e-payment systems, Electron. Commer. Res. Appl. 9 (2010) 84–95.
[91] Y. Lu, S. Yang, P.Y. Chau, Y. Cao, Dynamics between the trust transfer process and intention to use mobile payment services: a cross-environment perspective, Inf. Manag. 48 (2011) 393–403.

Obi Ogbanufe is currently a Ph.D. student in the Information Technology and Decision Sciences Department at the University of North Texas. She holds an M.S. in Systems Engineering and Management from the University of Texas at Dallas. Her research interests include information security, cybercrime, health information technology, and risk management.

Dan J. Kim is a Professor of Information Technology and Decision Sciences (ITDS) at University of North Texas (UNT). His research interests are in multidisciplinary areas such as information security and privacy, information assurance, and trust in electronic commerce. His research work has been published or in forthcoming >150 papers in refereed journals, peer-reviewed book chapters, and conference proceedings including *Information Systems Research, Journal of Management Information Systems, Communications of ACM, Communications of AIS, EJIS, DSS, International Journal of Human-Computer Interaction, Journal of Organizational and End User Computing, IEEE Transactions on Professional Communication, Electronic Market, IEEE IT Professional, Journal of Global Information Management, and International Journal of Mobile Communications, ICIS, HICSS, AMCIS, INFORMS, ICEC, ICA, and so on*. He has been awarded the National Science Foundation CyberCorps: SFS grant for multi-years, 2012 Emerald management Review Citations of Excellence Awards, 2010 Best Published Paper Award in ISR, an Emerald Literati Network 2009 - Outstanding Paper Award, the ICIS 2003 Best Paper-First Runner-up Award, and the AMCIS 2005 Best Research Paper Award at AMCIS 2005. He was ranked at 22nd worldwide in terms of research productivity from year 2008 to 2010 based on top three leading IS journals: ISR, MISQ and JMIS.

Please cite this article as: O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems (2017), https://doi.org/10.1016/j.dss.2017.11.003