Prof. Rachel Barker
Department of Communication Science, University of South Africa, Pretoria (barker@unisa.ac.za)

DOI: https://dx.doi.org/10.18820/24150525/Comm.v23.5
ISSN 2415-0525 (Online)
Communitas 2018 23: 71-86

KNOWLEDGE MANAGEMENT TO PREVENT FRAUDULENT E-BANKING TRANSACTIONS

ABSTRACT

The growth of e-banking as financial institutions encourage customers to do online banking transactions opened opportunities for criminals and sophisticated fraudsters to perpetrate and abuse customers in their social, cyber and physical worlds. This emphasises the need for communication and knowledge sharing by the financial service industry to empower customers in identifying dynamic fraud from genuine customer behaviour. The boundary of liability with respect to fraudulent e-banking transactions is shifting from the banking industry to the customer, with the emphasis on concepts like co-liability. Despite continuous efforts by the financial industry to increase customer awareness, the dominating lack of clarity about when clients have acted negligently has become problematic, which can lead to loss of customer trust and a demand for better security. This article addresses the lack of research on this through a critical analysis of knowledge management to enhance security and customer trust in e-banking. The study investigates fraud prevention and available e-security measures, the legal consequences on co-liability to negate these potential negative consequences to the benefit of both the financial industry and the customer, and proposes a conceptual theoretical framework for e-banking fraud prevention and co-liability through proactive communication.

Keywords: online communication; proactive communication; knowledge management; fraudulent e-banking transactions; e-security; customer trust; proactive communication of information; knowledge creation and sharing

INTRODUCTION

The following quote by Hoffman and Birnbrich (2012: 390) sets the scene for this research to develop a conceptual framework for fraud prevention in e-banking: “As banking fraud might ultimately affect customer relationship quality and customer loyalty, fraud prevention and its effective communication is an important topic for academic research”. According to Mhamane and Lobo (2012), e-banking, also known as electronic banking or internet banking (Yazdanifard *et al*. 2011), has become a prevalent mode for online and internet-based transactions.

E-banking offers a variety of banking services, including electronic transfer of funds (EFT), automatic teller machine (ATM) services and direct deposits automatic bill payment (ABP), a cheaper system when compared with traditional banking systems offering customers flexibility and comfortability (Yazdanifard *et al*. 2011). Despite its advantages, this considerable innovation opens up the possibility for fraudulent transactions and an intensification in cases of fraud associated with that present tremendous challenges to the banking sector to caution and inform customers who do not use this service due to fears. It also provides fraudsters with more opportunities to attack customers, especially because they are not physically present to authenticate transactions, and might even facilitate organised attacks.

According to Van der Meulen (2013: 713), this fraud is among the most lucrative types of cybercrime in contemporary society. According to Wei *et al*. (2013), e-banking fraud reflects the synthetic and integrative abuse on the interaction between resources, which includes the fraudster's intelligence abuse in the social world, the abuse of internet banking resources and technology in the cyber world, and the abuse of trading tools and resources in the physical world. The results of a study conducted by Carminati *et al*. (2015: 176) highlighted the significant growth of online or e-banking fraud, fuelled by the underground economy of malware. According to them, internet banking frauds are difficult to detect because the fraudulent behaviour is dynamic, spread across different customer profiles, and dispersed in large and highly imbalanced datasets (e.g. web logs, transaction logs, spending profiles).

Although the phenomenon of a "zero tolerance co-liability process on fraudulent banking transactions" is mentioned in current literature to prevent or negate potential negative consequences, this phenomenon has not been adequately researched, understood and conceptualised as a prevalent aspect of shared responsibility to the benefit of both the financial industry and the customer. In order to gain academic insight into this phenomenon, this study sets out to investigate the means by which fraudulent activities in e-banking are committed and the way in which the financial sector addresses this through the introduction of security measures, education, awareness and the management of knowledge through proactive communication to increase customers' loyalty and trust and at the same time to enhance the bank's reputation and customer retention. The theoretical discussion will be based on an extensive literature search using these concepts and inclusion and exclusion criteria. The problem statement for this research is that there seems to be no theoretical framework to address the applicability of the identified and characterised theoretical typologies derived from the knowledge management paradigm and e-banking fraud to elaborate on the need to enhance e-security and customer trust.

KEY CONCEPTS

Fraudulent e-banking transactions

Fraudulent e-banking transactions are among the most money-spinning types of cybercrime today. According to Van der Meulen (2013: 713), the increased sophistication of attacks has complicated prevention and detection efforts, which in turn has allowed their success to proliferate. This has increased the financial burden on both the service providers and the customers, where the latter are running increasing legal risks of being exposed to financial losses due to neglect. The internet is an effective communication device or tool for providing proactive customised and personalised delivery of interactive messages. Jansen and Leukfeldt (2015: 31) emphasise the need to educate online banking customers about how to avoid fraudulent schemes.

According to Andrews and Boyle (2008: 60), the main inhibiting factor for many forms of transactions is that of perceived risk, especially in e-banking, which influences customer's perceptions and behaviour to adopt or reject these offerings. Various viewpoints exist on perceived risks depending on the predefined perspectives of the researchers to reflect the particular context under examination. Because the purpose of this study is to examine the need to enhance security and customer trust in e-banking, the focus will be on security measures, proactive communication on possible risks of fraudulent transactions and how to educate customers through knowledge sharing on fraud prevention and the consequences of neglect. This type of perceived risk is defined by Sathye (1999: 326) as the security and reliability of transactions; moreover, the risk of losing money through fraudulent transactions or that personal information might be misused (Drennan *et al*. 2006).

Security measures for fraud detection and fraud prevention

The two main approaches used by the banking industry to detect fraud patterns include tapping the data warehouse of the third-party (containing transaction information from many institutions) by using data mining programmes to identify fraud patterns and fraud pattern identification, which is based stringently on the bank's own internal information (mostly through a hybrid approach) (Bhasin 2015). Most fraud detection methods are related to credit card fraud, computer intrusion and mobile communication. Empirical analysis performed on real-world transactions revealed that most of the fraud had the following characteristics: a large number of different accounts accessed by a single fraudster; transactions involving small values in many accounts; more payment transactions than usual in a single account; and an increased number of login and password failures before the occurrence of fraud (Kovach & Ruggiero 2011).

Fraud prevention, on the other hand, describes the security measures to avoid unauthorised individuals from initiating transaction on an account for which they are not authorised (Kovach & Ruggiero 2011: 166). When fraud prevention for e-banking transactions fails, fraud detection is used to identify this unauthorised activity. The need for security is therefore a fundamental and increasingly important issue in the banking industry, which highlights the need for fraud prevention through proactive communication to ensure customer relationship quality and loyalty (Hoffman & Birnbrich 2012). Due to a lack of research on fraud prevention, it will be the focus of this study.

Customer co-liability

Although the general assumption is that customers are not liable and that banks refund the financial losses of victims of e-banking fraud, the banking industry is moving towards customer co-liability and is investigating the need for a zero-tolerance policy through increased efforts to educate and train customers proactively. According to Van der Meulen (2013: 718), and based on cases worldwide, trying to introduce a zero (co)liability policy, it can negate potentially negative consequences, by eliminating the uncertainty for consumers and simultaneously making discussions on clarity and constancy obsolete. Due to the increase in fraudulent e-banking transactions, banks are starting to expect more from customers in response to years of awareness campaigns and argue that they count on a certain level of awareness that can be used as a vehicle to transfer the liability from the side of the bank to the customer.

This is hampered by two concerns. Firstly, there is the lack of clarity on the qualification of gross negligence and care, which can be open to interpretation. To address this concern, banks argue that the specificity of a warning allows for the transfer of liability to the customer. In other words, if perpetrators use a “known” attack that clients were warned against, and are successful, then the customer acted negligently and should be liable. This leads to the second concern of consistency, causality and reasonableness where the liability can be circumstantial (for example, if any form of social engineering was absent, lines of liability were not specified, burden of proof for customers and banks, etc.). One line of liability, which clients agree to in terms of use by opening and subsequently using the account, is the installation of antivirus software (usually provided by the bank online free of charge). In addition, ignoring the warnings of malware and phishing/vishing by clicking on links and responding to emails are serious fraud threats, but the inclusion of more specific terms of use might reduce the lack of clarity and consistency as banks will then be more transparent about their expectations.

Customer trust

Trust is a decisive instrument in stimulating purchasing over the internet and is a determining factor whether customers will accept e-banking. Yousafzai *et al*. (2003) refer to two types of trust in e-banking: the traditional perspective of trust in a specific party (the bank), and trust in the integrity of the transaction medium (the web). According to Yazir and Majid (2017), trust depends on information and knowledge sharing, whilst Reichheld and Schefter (2000) consider e-trust as the degree of confidence customers have in online exchanges in e-banking.

There are arrangements with customers that can increase trust and belief in relation to the bank and its intentions. They include reading security declarations and accepting them; enhancing communication and transparency about the bank in terms of fraud and security; clarifying security expectations; refund arrangement effectiveness; introducing layered security strategies and solutions to ensure proactive security and comfortability to use it; and differentiating between fundamental and legitimate activities that provide the highest degree of protection without overburdening. Prevention tips and enhancing security in e-banking is not an easy task for banks because most of the attacks have already occurred before the banks realise it. However, they do have the following control prevention methods in place: KeCrypt - not possible to forge, fake or fool; multifactor authentication; new users who approve or request large transfers are immediately associated with high-risk behaviour and should be acted upon immediately; and Spyware Protection through built-in antispyware (a personal firewall is another way to do this). Most financial institutions apply these prevention methods and have come up with innovative approaches to develop and enhance trust with customers through proactive communication and education.

Effective knowledge management through proactive communication on anti-fraud management enhances customer relationships and ultimately loyalty and trust (Hoffman & Birchman 2012). In the context of this study, customer relationships refer to the relationship the bank builds with the customer where the quality of this relationship is dependent on the loyalty and trust of the customer towards the bank. For the purpose of this study, relationship quality is defined as the strength of the relationship to create, maintain and enhance the satisfaction, trust and commitment of the customer to enhance long-term customer relationships. According to Liu *et al*. (2011) and Randall *et al*. (2011), satisfaction refers to the evaluation of customers on products and services based on past experience, expectations, predictions, goals and desire to assess the quality of past interactions. Ghane *et al*. (2011) argue that customer satisfaction is closely related to interpersonal trust and can be considered as an antecedent of e-trust and e-loyalty to ensure customers have the intention to revisit the website and make future transactions.

In terms of fraudulent e-banking transactions, satisfaction of interactions will foster customer intention to continue using these services (Ho & Ko 2008). In a study conducted by Hoffman and Birnbrich (2012), they concluded that reliable and regular communication about fraud and the systems, methods and measures that are taken to prevent it will, inter alia, lead to increased levels of satisfaction, knowledgeable customers on anti-fraud measures, and fraud prevention that is positively associated with trust and commitment. This will ultimately lead to loyalty and successful long-term relationships.

THEORETICAL FRAMEWORK

Based on the pragmatic realist approach of Miles *et al*. (2013:7) that there are regularities and sequences that link together phenomena from which constructs can be derived that underlie individual and social life, they posit that human relationships and societies have peculiarities and inconsistencies that make a realist approach to understanding them more complex – but not impossible. They agree with interpretivists that knowledge is a social and historical product and affirm the existence of the subjective, phenomenological and meaning as the centre of social life and that these processes should be transcended into theories to account for a real work and to test these theories in practice. This article follows a social science perspective, specifically communication science, focusing on individuals (not a computer science perspective concentrating on technological fixes or psychological approach converging on behaviour) through an exploratory, descriptive and critical analysis of existing information based on an interpretative approach.

The accelerated capacity of online transactions and e-banking can either empower an individual or counteract the threats posed by the increasing fragmented media landscape and emergence of independent online media outlets. One way to counteract this is to engage with the online community using proactive knowledge management communication by incorporating safety and security messages on the website to warn and reassure customers of prevalent fraudulent transactions. This emphasises that banks should put in place incentives, systems, methods and measures that are more robust to provide for the security of customers' accounts if they want to impose liability from a legal perspective. Because knowledge management is a multifaceted socio-technical process encompassing various forms of knowledge creation, storing, representation and sharing to the benefit of the organisation and its individuals, it is seen as information with specific properties and the introductory stage to knowledge (Lueg 2001). Contained in this definition are three key components of the knowledge management process relevant to this study: technology (web), human (customer), and organisation (banks). Technology focuses on data gathering, mining and knowledge construction. The human component refers specifically to the knowledge creation and sharing of information through online messages during direct, real-time interactions. The organisational component includes the management of four interrelated elements: choice, adoption and implementation of procedures/methods to link individuals and groups; formal and informal informational settings where interaction occurs; organisational practices to address fraud; and the context in which interactions and messages are facilitated.

The knowledge management theory is becoming more and more popular to study the proactive management of online communication as one way of facilitating messages to prevent fraudulent e-banking transactions. This theory has received recognition since the mid-1990s. Earlier knowledge management studies focused mainly on the capture and dissemination of knowledge. Since the mid-1990s, the focus shifted towards the CoP ideas, which led to the first community of practice (or communities of knowledge sharing) that emerged in 1997, and in the virtual world refers to VcoPs (Barker 2006).

Although most traditional approaches to knowledge management assumed this knowledge as relatively simple, approaches that are more recent realise that knowledge is in fact complex, factual, conceptual and procedural. A tendency still exists to follow the tradition in thinking of communication as the transfer and processing of information, but more recently the focus is on proactively communicating with customers through the creation and sharing of knowledge (Donate & De Pablo 2015; Barker 2016). One of the key discourses of the knowledge management paradigm is that embodied, tacit, implicit and narrative knowledge are important phenomena and fundamental to all human knowing (Nonaka & Takeuchi 1995) and an essential part of everyday communication because it allows for the transformation, sharing and processing of knowledge (Barker 2009).

The starting point of this study is therefore evidenced in the processes of knowledge management as a comprehensive approach to online communication in general, and in this article particularly with regard to proactive communication on fraudulent e-banking transactions. This is necessitated by the realisation of substantial operating costs for banks to refund customers' monetary losses (Gates & Jacob 2009), as well as the considerable time and emotional loss of customers. Customers have to detect the fraudulent transaction, communicate with the bank, initiate blocking and re-issuing or re-opening a card or account, and dispute the reimbursement of losses (Douglass 2009; Malphrus 2009). The consequences for the bank is shattered trust and confidence, a feeling of insecurity, a lack of confidence and increased dissatisfaction because of a perceived service failure, which in turn affects loyalty and damages the bank's reputation (Gruber 2011).

Greer and Moreland (2003) suggest that effective [online] communication requires customised content-based messages to warn and educate customers of potential e-banking fraudulent transactions. It also gives banks the opportunity to (re)assure customer trust in their services and allows a bank to evoke a shared understanding of values between itself and its customers (Asif & Sargeant 2000) to retain existing and/or attract new customers. Knowledge management also allows banks to demonstrate their knowledge and competence regarding anti-fraud measures effectively, thereby creating a feeling of safety among customers that can improve customer relationship quality and loyalty (Hoffman & Birnbrich 2012). If applied to e-banking to create awareness for the prevention of fraudulent banking, it is argued that the knowledge management paradigm presents a way to proactively manage and control the messages that are acquired, transferred and assimilated.

PREVENTION OF E-BANKING FRAUD

Against the background that internet or e-banking fraud is difficult to detect and analyse, it is argued that it is better to communicate with and educate customers to create awareness and knowledge through proactive knowledge management and knowledge sharing. This will allow banks and customers to build commonality and trust on the prevention of fraudulent banking transactions and move towards co-liability and ultimately a zero-tolerance policy. This will narrow the gap between bank-wise (globally) and user-wise (locally) attribute distributions who will become well-trained users on fraud (Carminati *et al*. 2015).

Categories of fraud

In the literature, the person conducting it categorises fraud. Two types of fraud are identified. First-party fraud is when a legitimate customer betrays the bank; and third-party fraud is when the customer becomes a victim of criminals who steal identities, the use of lost or stolen cards, counterfeit cards, or gain unauthorised access to customer accounts by any other means (Gates & Jacob 2009; Greene 2009).

This study focuses on the prevention of third-party fraud that falls into two categories. Firstly, there is payments fraud that refers to any activity that uses information from any type of payments transaction for unlawful gain and occurs when fraudsters gain access to and use customers' accounts for their own financial benefit. Secondly, there is identity theft, which might include fraudsters illicitly gaining access to customer accounts, but mostly refers to the opening of new accounts in the name of a customer (Malphrus 2009; Hoffman & Birnbrich 2012; Sullivan 2010; Gates & Jacob 2009).

In the context of this study, the prevention of fraud describes the security measures to avoid unauthorised individuals from initiating transactions on an account for which they are not authorised (Kovach & Ruggiero 2011: 166). One way to do this is to focus on the regulated financial institutions who must consider the security of service providers. These include, inter alia, new laws and systems, methods and standards for payment activities and instruments, whether new payment types carry an excessive fraud risk, who is liable when fraudulent payments occur, how losses are located, what customer protection should be in place, how notification of fraud should be handled, and how to minimise the incidence of fraud (Gates & Jacob 2009). On the other hand, the move towards co-liability introduces the need to manage knowledge and information on fraudulent banking transactions through proactive communication with customers to create awareness, educate, and at the same time introduce them to the concept of co-liability.

Types of fraudulent e-banking transactions

Based on the literature, fraudulent processes entail giving away personal information to fraudsters through phishing/vishing or malware victimisation. Phishing/vishing victimisation is defined by Lastdrager (2014: 8) as a "scalable act of deception whereby impersonation is used to obtain information from a target". It occurs when customers respond to a false email, a fraudulent phone call, or a combination. Fraudsters then "steal" access data by pretending to be a credible source requesting sensitive information like usernames or passwords (Hoffman & Birnbrich 2012). Malware victimisation is the umbrella term for malicious software such as viruses, worms, Trojan horses and spyware to steal credentials or digital data, or gain control over a customer's screen (Jansen & Leukfeldt 2015: 24). This usually occurs by responding to a pop-up message and by installing a malicious application of a mobile device or banking app.

Despite various awareness campaigns, customers still tend to be ignorant and do not read or pay attention to information on their screens that might have prevented the fraudulent transaction and/or that they were not mentally able to stop the process because of trusting the intention of the fraudster. According to Yazdanifard *et al*. (2011), the cybercrime trends created by malware, specifically Trojans, are programmes that compromise the computer without the knowledge of the user. The number one worldwide-recognised malware in e-banking fraud, according to these authors, is known as the Zeus Trojan 'defacto' where Zeus has become almost like a brand version of a Trojan (*ibid*.).

Characteristics of e-banking fraud

The most sophisticated characteristics of e-banking fraud are summarised by Wei *et al*. (2013: 450) as follows: suspicious customers are active and intelligent in conducting fraudulent e-banking transactions; fraudulent behaviour is dynamic; fraud is hidden in diversified customer behaviour; fraud-related transactions are dispersed in highly imbalanced large data sets; and the occurrences of fraud appear in a very limited time which requires real-time detection. These aspects focus on fraud detection, not prevention, but they are mentioned for contextualisation purposes of the need for advances in e-security measures.

Fraud legislation

In a study conducted by Mason and Bohm (2017) in the United Kingdom on the scale of bank-transfer fraud and the cost for customers to take action, they proposed various new measures and greater liability for banks to ensure that customers are protected by law. One such liability is described as "security updates" to prevent fraud, especially the legal issue which is straightforward: whether the bank had the authority under its mandate from the customer to debit the account. For example, if a card is used at an ATM and the correct PIN is entered, the bank can claim that it was the customer or a person authorised by the customer. According to Chavan (2013), fraudulent e-banking transactions need to have a legal definition, recognition and permission if new methods and instruments are developed and implemented.

Potential consequences of a co-liability process

Customers who become a victim of fraud are negatively affected in various ways (Malphrus 2009; Button *et al*. 2014; Hoffman & Birnbrich 2012). Firstly, monetary losses, even though it is typically refunded by banks. Secondly, time in terms of the efforts customers have to make to restore the original situation. Thirdly, customers might lose confidence and trust in the bank and feel that it is not safe and that the bank is incapable of protecting their assets and might want to switch to another bank. These accumulated e-banking fraud incidents ultimately have a profound negative impact on the reputation of the bank. Based on the literature, the potential negative consequences for both the customer and bank indicated in Table 1 are prevalent if customers are held liable for internet banking usage in general and fraudulent e-banking transactions specifically (Van der Meulen 2013; Hoffman & Birnbrich 2012; Tassabehji & Kamala 2012; Yazdanifard *et al*. 2011; Jansen & Leukfeldt 2015; Chiou & Shen 2012).

These concepts can typically be viewed in terms of three notable influences of the online environment on communication, namely, time and space compression, global consciousness and reflexivity, and disembeddedness in single locations (Monge 1999). In the context of this study, time and space compression refers to the physical or "real" presence through new technologies; in this case e-banking, which links customers who are removed from the bank to communicate as if they are in a single location. In terms of global consciousness, new technologies allow customers access to stored information and knowledge in local and international repositories and security websites through an interchangeable process. Disembeddedness in a single location aids in the reconnection of individuals at a distance by distributing knowledge through information to increase knowledge levels, thereby creating a new space – albeit not a physical space – in which customers feel safe. This re-emphasises the need for increased security and trust in e-banking.

TABLE 1: POTENTIAL CONSEQUENCES OF A CO-LIABILITY PROCESS

BANKS		**CUSTOMERS**
Positive	Monetary savings/less cost	Increased awareness
	Clarity and consistency of definitions of concepts such as gross negligence	Less time-consuming to react to fraud
	Less obligation ('back door escape')	Access to security methods and systems (antivirus software, security centres, etc.)
	Increased transparency	More knowledgeable on security and fraud through education
	Retain customers	Increased interaction with banks
Negative	Refusal to refund can lead to negative publicity	Perceived risk and uncertainty (security/privacy, financial, social, time/ convenience and performance risks)
	Loss of trust, loyalty, commitment, etc.	Demand for better e-security
	Lose customers	Concerns about cybercrime inhibits online participation (inconvenience)
	New methods/systems a costly investment (for example, the usage of biometrics)	No refunds problematic and cause for concern (financial loss)

Actions to be considered in new policies, measures and procedures

Mason and Bohm (2017: 240) consider the following actions necessary by banks to enhance trust and responsibility. Firstly, the government must change rules for reporting and dealing with theft from bank accounts and provide accurate figures on theft and fraud. Secondly, training, education and provision of appropriate information technology to security staff on digital criminal activities is crucial. Thirdly, banks must put more robust methods in place to provide security to customers with relevant incentives. Fourth, consideration must be given to the general rule that machines may be assumed to work correctly, which ignores the susceptibility of commercial software being manipulated to the detriment of the customer. Lastly, the problem should be treated less simplistically by the banks and it ought to be a requirement to inform customers that their accounts have been compromised.

A CONCEPTUAL THEORETICAL FRAMEWORK FOR FRAUDULENT E-BANKING TRANSACTIONS

A conceptual framework explains, either graphically or in narrative form, the key constructs, variables or factors that need to be studied and the presumed interrelationship between these (Miles *et al*. 2013). For the purpose of this study, a graphical conceptual framework is developed based on the current version of the researcher's map obtained from a comprehensive literature review and the important variables identified in the qualitative research. Based on the preceding literature review and key theoretical constructs of the knowledge management process and variables identified from existing literature, Figure 1 proposes a conceptual theoretical framework for e-banking fraud prevention and co-liability through proactive communication.

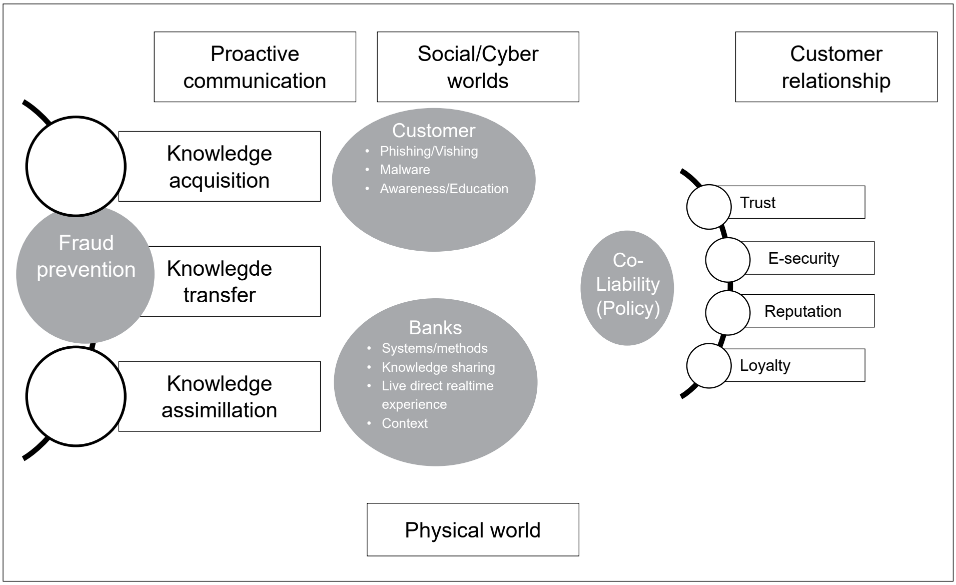

FIGURE 1: CONCEPTUAL FRAMEWORK FOR E-BANKING FRAUD PREVENTION AND CO-LIABILITY THROUGH PROACTIVE COMMUNICATION

The focus in this conceptual framework is on fraud prevention using the three typologies of knowledge management to communicate with customers proactively. In this context, knowledge acquisition refers to the provision of instructing information on the website to customers when a new fraudulent action is identified and/or to remind them of existing methods and procedures. It encompasses data gathering and mining as well as knowledge construction. Three main types of messages should be constructed: basic facts about fraud; updating of existing information and facts; and provision of new information and messages to prepare customers for what to expect and how to react to it. This is usually done through a security centre website, pop-ups to warn customers when they access their accounts, and detailed links to cover the broad spectrum and context of fraudulent transactions.

Knowledge transfer is necessary to move into creating and adjusting the communication messages by posting various messages and linking customers to websites for direct real-time interactions and by sharing information to ensure them of the safe and secure use of online transactions. Examples of possible real-time fraudulent transactions should be included on various websites and links to transfer this knowledge to the customer.

Knowledge assimilation should be substantiated through the control and management of the messages in the pre, present and post stages of fraudulent actions by presenting methods and procedures to ensure safe e-banking transactions, providing informal and formal settings for interaction (for example, hotlines and online links), stating company practices to address fraud and the context in which it is managed and controlled. This is usually corroborated through linking customers to the security centre, online fraud updates, media releases, general security messages (formal or informal), and detailed methods, practices and procedures to address it proactively and reactively.

It is argued that the knowledge management paradigm offers the opportunity to manage and control proactive communication by means of these typologies through a series of messages and links to assure customers of safe and secure online transactions. These typologies should be used consistently and continuously to create awareness of fraudulent banking transactions in the social, cyber and physical worlds of both the customer and the banks. Customers should be educated to create awareness on phishing/vishing and malware fraudulent banking transactions to prevent these actions. Banks should constantly provide systems and methods and prompt customers on existing and/or new fraudulent transactions to ensure that the concept of "zero-tolerance liability" becomes a crucial concept in the prevention of fraudulent e-banking transactions.

The starting point of this study is therefore evidenced in the processes of knowledge management as a comprehensive approach to online communication in general, and in this article particularly with regard to fraudulent e-banking transactions. In terms of the theoretical discussion of the knowledge management paradigm, the following three major typologies indicated above are relevant to this study:

- Firstly, to acquire knowledge through data mining and knowledge construction to address it proactively (whether empathic, reminders against complacency, and to address ambiguity and uncertainty).
- Secondly, adequate response and attitude towards fraudulent e-banking transactions by means of the transfer of knowledge to customers through the creation and sharing of knowledge in direct real-time interactions (e.g. setting the customers' mind at ease and ensuring them of the safety and security of online transactions).
- Thirdly, the assimilation of knowledge to address current fraudulent e-banking issues and to present methods and procedures to link customers to possible preventative or corrective actions to ensure authenticity and transparency in the trust-building process (e.g. through downloading of free software, steps or guidelines to ensure safe and secure use of online transactions, reduced risk strategies, and media releases).

Although it is realised that the main advantages created by e-banking is the ease of use any time and any place, no barriers to access, convenience, and the minimal cost of services, it is also posited that the application of the constructs in the conceptual theoretical framework will introduce customers to the importance of co-liability without losing trust, commitment or loyalty, or impact negatively on the reputation of the banks.

CONCLUSION

By adopting a knowledge management approach, the study examined the importance of the management and control of messages on fraudulent e-banking transactions. This often results in the construction of opposing viewpoints, but a way to ameliorate this tendency is to promote the recognition of the fraud and proactively communicate messages to alleviate concerns and ensure customers of the safe and secure use of online transactions. This emphasis on the managing of messages resonates with the knowledge management paradigm and implies that online knowledge creation and sharing can be constructed and controlled through the three identified typologies: knowledge acquisition, transfer, and assimilation.

The majority of banks are beginning to exploit their information "asset" for deriving of fraudulent e-banking transactions through data mining to gain a competitive advantage. Customer retention and acquisition became an important determinant of a bank's bottom line and if these typologies are applied in decision-making, they can reap immense benefits and derive considerable competitive advantage to withstand competition in future. The introduction of a zero-tolerance and/or co-liability policy or measures in future necessitates the need for banks to continue monitoring fraudulent transactions, and to proactively communicate and educate customers to ensure positive customer relationships and trust. The boundary of liability will also force banks to become more transparent and harmonise liability rules to enhance clarity and consistency between banks on gross negligence.

It was argued that the boundary of liability with regard to online banking fraud is gradually starting to shift from the bank to the customer and despite various awareness campaigns to educate and introduce such a shift, the increase in sophisticated fraud attacks makes customers vulnerable to the "involuntary facilitation" of fraud. Hence, Van der Meulen (2012: 717-718) posits that the introduction of a genuine zero liability policy can negate these potentially negative consequences by removing the uncertainty for consumers and simultaneously making discussions on clarity and consistency obsolete. It is concluded that this conceptual framework be tested empirically to obtain a deeper understanding of and account for the influence of control and management of messages on e-banking fraud to address issues like perceived risk, trust and customer relationships. The importance of the technology, human and organisation typologies of the knowledge management approach is accentuated by the following quote: "Sophisticated online banking fraud involves multiple resources, including human wisdom, computing tools, web technology and online business systems" (Wei *et al*. 2013: 472).

REFERENCES

Andrews, L. & Boyle, M.V. 2008. Consumers' accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal* 11(1): 59-75. https://doi.org/10.1108/13522750810845559

Asif, S. & Sargeant, A. 2000. Modelling internal communications in the financial services sector. *European Journal of Marketing* 34(3/4): 299-317. https://doi.org/10.1108/03090560010311867

Barker, R. 2006. The virtual reality of knowledge creation in cyberspace: a knowledge management perspective. *Conference Proceedings, 2nd Biennial Conference of the Academy of World Business, Marketing and Management Development* 2(1): 132-142.

Barker, R. 2009. A study of knowledge creation and management in virtual communities. *The Journal of Management and World Business Research* 6(1): 1-17.

Barker, R. 2016. Knowledge management as change agent to ensure the sustainability of emerging knowledge organisations. *Proceedings of the 17th European Conference on Knowledge Management,* 1-2 September 2016, Belfast, Ireland.

Bhasin, M.L. 2015. Data mining: A competitive tool in the banking and retail industries. *The Chartered Accountant* October 2015: 588-594.

Button, M., Lewis, C. & Tapley, J. 2014. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27(1): 36-54. https://doi.org/10.1057/sj.2012.11

Carminati, M., Toberto, C., Maggi, F., Epifani, I. & Zanero, S. 2015. Bank Sealer: A decision support system for online banking fraud analysis and investigation. *Computers and Security* 3: 175-186. https://doi.org/10.1016/j.cose.2015.04.002

Chavan, J. 2013. Internet banking benefits and challenges in an emerging economy. *International Journal of Research in Business* 1(1): 19-26.

Chiou, J.S. & Shen, C.C. 2012. The antecedents of online financial service adoption: The impact of physical banking services on Internet banking acceptance. *Behaviour and Information Technology* 31(9). https://doi.org/10.1080/0144929X.2010.549509

Donate, M.J. & De Pablo, J.D.Z. 2015. The role of knowledge-orientated leadership in knowledge management practices and innovation. *Journal of Business Research* 68: 360-370. https://doi.org/10.1016/j.jbusres.2014.06.022

Douglass, D.B. 2009. An examination of the fraud liability shift in consumer card-based payment systems. *Economic Perspectives* 33(1): 43-9.

Drennan, J., Sullivan Mort, G. & Previte, J. 2006. Privacy, risk perception and expert online behaviour: An exploratory study of household end-users. *Journal of Organisational and End User Computing* 18(1): 1-21. https://doi.org/10.4018/joeuc.2006010101

Gates, T. & Jacob, K. 2009. Payments fraud: perception versus reality – a conference summary. *Economic Perspectives* 33(1): 7-15.

Ghane, S., Fathian, M. & Gholamian, M.R. 2011. Full relationship among e-satisfaction, e-trust, e-service quality and e-loyalty: The case of Iran e-banking. *Journal of theoretical and applied information technology* 33(1): 1-10.

Greene, M.N. 2009. Divided we fall: fighting payments fraud together. *Economic Perspectives* 33(1): 37-42.

Greer, C.F. & Moreland, K.D. 2003. United Airlines' and American Airlines' online crisis communication following the September 11 terrorist attacks. *Public Relations Review* 29(4): 427-441. https://doi.org/10.1016/j.pubrev.2003.08.005

Gruber, T. 2011. I want to believe they really care: How complaining customers want to be treated by frontline employees. *Journal of Service Management* 22(1): 85-110. https://doi.org/10.1108/09564231111106938

Ho, S. & Ko, Y. 2008. Effects of self-service technology on customer value and customer readiness: The case on Internet banking. *Internet Research* 18(4): 427-446. https://doi.org/10.1108/10662240810897826

Hoffman, A.O.I. & Birnbrich, C. 2012. The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *International Journal of Bank Marketing* 30: 390-407. https://doi.org/10.1108/02652321211247435

Jansen, J. & Leukfeldt, R. 2015. How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Workshop on Socio-Technical Aspects in Security and Trust (STAST).* Electronic ISSN: 2325-1697

Kovach, S. & Ruggiero, W.V. 2011. Online banking fraud detection based on local and global behaviour. *ICDS 2011: The Fifth International Conference on Digital Society.* IARIA.

Lastdrager, E.E.H. 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Scene* December 2014: 3-9.

Liu, C.T., Guo, Y.M. & Lee, C.H. 2011. The effects of relationship quality and switching barriers on customer loyalty. *International Journal of Information Management* 31(1): 71-9. https://doi.org/10.1016/j.ijinfomgt.2010.05.008

Lueg, C. 2001. Information, knowledge and networked minds. *Journal of Knowledge Management* 5(2): 151-159. https://doi.org/10.1108/13673270110393194

Malphrus, S. 2009. Perspectives on retail payments fraud. *Economic Perspectives* 33(1): 31-6.

Mason, S. & Bohm, N. 2017. Banking and fraud. *Computer Law and Security Review* 33(2): 237-241. https://doi.org/10.1016/j.clsr.2016.11.018

Mhamane, S. & Lobo, L.M.R.J. 2012. Fraud detection in online banking using HMM. *International conference on information and network technology (ICINT)* 37: 200-203.

Miles, M.B., Huberman, A.M. & Salandha, J. 2013. *Qualitative data analysis: a methods sourcebook.* (Third edition). Los Angeles: Sage.

Monge, P.R. 1999. Communication structures and processes in globalisation. *Journal of Communication* 9(3): 142-153.

Nonaka, I. & Takeuchi, H. 1995. *The knowledge-creating company: How Japanese companies create the dynamics of innovation.* New York: Oxford University Press.

Randall, W.S., Gravier, M.J. & Prybutok, V.R. 2011. Connection, trust, and commitment: dimensions of co-creation? *Journal of Strategic Marketing* 19(1): 3-24. https://doi.org/10.1080/0965254X.2010.537760

Sathye, M. 1999. Adoption of Internet banking by Australian consumers: An empirical investigation. *International Journal of Bank Marketing* 17(7): 324-5. https://doi.org/10.1108/02652329910305689

Sullivan, R.J. 2010. The changing nature of U.S. card payment fraud: industry and public policy options. *Economic Review* 95(2): 101-33.

Tassabehji, R. & Kamala, M.A. 2012. Evaluating biometrics for online banking: The case for usability. *International Journal of Information Management* 32(5): 489-494. https://doi.org/10.1016/j.ijinfomgt.2012.07.001

Van der Meulen, N.S. 2013. You've been warned: Consumer liability in internet banking fraud. *Computer and Security Review* 713-718.

Wei, W., Li, J., Cauo, L., Ou, Y. & Chen, J. 2013. Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web* 16: 449-475. https://doi.org/10.1007/s11280-012-0178-0

Yazdanifard, R., Yosoff, W.F.W., Behora, A.C. & Sade, A.B. 2011. Electronic banking fraud: The need to enhance security and customer trust in online banking. *International Journal in Advances in Information Sciences and Services and Sciences* 3(10.61): 505-509.

Yazir, M. & Majid, A. 2017. Impact of knowledge management enablers on knowledge sharing: Is trust a mission link in SMEs of emerging economies? *World Journal of Entrepreneurship, Management and Sustainable Development* 13(1): 16-33. https://doi.org/10.1108/WJEMSD-02-2016-0010

Yousafzai, S.Y., Pallister, J.G. & Foxall, G.R. 2003. A proposed model of e-trust for electronic banking. *Technovation* 23(11): 847-860. https://doi.org/10.1016/S0166-4972(03)00130-5