AWARENESS CREATION ON E-BANKING FRAUD PREVENTION: A KNOWLEDGE MANAGEMENT PERSPECTIVE FOR E-SECURITY AND CUSTOMER RELATIONSHIP BUILDING

Rachel BARKER
University of South Africa
P.O. Box 395, Pretoria, 0003, Republic of South Africa
barker@unisa.ac.za

Abstract: *E-banking, also known as electronic or Internet banking, has become a prevalent mode for online and internet-based transactions. However, modern databases, online information and knowledge sharing, and increased access points for e-banking transactions opened opportunities for sophisticated fraudsters to perpetrate and abuse customers in their social, cyber and physical worlds. The intensification in cases of fraud presents tremendous challenges for the banking sector to caution, educate and inform customers on cybercrime because it reflects the synthetic and integrative use of the interaction between resources which include the fraudster's intelligence abuse in the social world, the abuse of knowledge resources and technology in the cyber world and the abuse of resources and trading tools in the physical world. Most studies focus on the detection of fraud patterns through tapping in data warehouses of third-party or by using data mining programs to identify fraud patterns, specifically credit cards, computer intrusion and mobile communication or first-party fraud when a legitimate customer knowingly betrays the bank. This study focuses on the prevention of fraud that falls into two main categories, namely: phishing/vishing/SMishing and malware practices (any activity of payment fraud where fraudsters gain access and uses customer' accounts for their own unlawful financial benefit); and identity theft (gaining access to or opening new accounts in the customer's name). The main premises of the research problem are built on the fact that a lack of studies exists to investigate the use of proactive communication through the three typologies of knowledge management to create awareness and educate customers on e-security measures and prevention of e-banking fraud where the move towards (co)liability should not impede but enhance customer relationship building. The research is conducted through a qualitative research methodology and the subject under study was the website of the South African Banking Risk Information Centre (SABRIC) purposefully sampled. The three concurrent cyclical flow of activity of the data analysis interactive model was used in the research. An abductive approach was used to report on the findings based on descriptions and interpretive comments relating it to and drawing on the theoretical thrusts identified. Main findings suggest, inter alia, the importance to proactively educate customers on how to protect themselves before they fall, victim, the importance of visibility on security measures, methods and standards for e-banking, and the move towards a (co)liability policy and shared responsibility process.*

Keywords: *Knowledge management; knowledge sharing; e-banking security; fraudulent e-banking transactions; customer relationships.*

Introduction

Despite the continuous efforts of the financial industry to increase consumer awareness on fraudulent e-banking transactions, the dominating lack of clarity about when precisely clients have acted negligently by denying to refund them has become problematic, which can lead to a demand for better e=security to ensure customer relationship building. According to Mhamane and Lobo (2012), e-banking has become a prevalent mode for both online and Internet-based transactions resulting in an intensification in cases of fraud associated with it. It provides fraudsters with more opportunities to attack customers, especially because they are not physically present to authenticate transactions and might even facilitate organized attacks (Barker, 2016). The results of a study conducted by Carminati et al. (2015, p.176) highlighted the significant growth of e-banking frauds, fueled by the underground economy of malware. According to them, Internet banking frauds are difficult to detect because the fraudulent behavior is dynamic, spread across different customer profiles and is dispersed in large and highly imbalanced datasets (e.g. weblogs, transaction logs, spending profiles). These results set the scene for this study to investigate the need for proactive communication and education of customers to create awareness on the prevention of fraudulent e-banking transactions through knowledge management (KM) and knowledge sharing to caution and inform them on the move towards (co)liability in cases of neglect. The dynamics of e-banking transactions in a virtual environment is not a narrow issue that only applies to online communication. Although recent research focuses strongly on fraud detection measures and patents (Leite et al., 2018, p.333), limited research is conducted on fraud prevention. Consequently, the purpose of this study is to test a conceptual framework developed from a combination of different viewpoints to identify and discover different types of frauds and to examine how Africa's trusted financial crime risk information center leveraging on strategic partnerships used their website as one way for fraud prevention by conveying information following fraudulent e-banking transactions.to proactively manage and/or prevent customers to fall victims to these fraudulent actions. Specifically, the study focuses on the way in which KM, through change agents or communication 'experts', can create a positive effect towards e-banking transactions through the control of messages in fraud prevention. For the purpose of this study "fraud prevention describes the security measures to avoid unauthorized individuals from initiating a transaction on an account for which they are not authorized" (Kovach & Ruggiero, 2011, p.166).

The paper is structured as follows. Firstly, a synopsis of the theoretical underpinning based on an extensive literature review is presented with a specific focus on fraudulent e-banking transactions, customer (co)liability, e-security and customer relationship building. Secondly, the theoretical research framework is proposed. Thirdly, the methodology, data analysis, and results are presented. Finally, a discussion of the main results based on the knowledge management typologies which can be used to manage and control fraud prevention are described.

Key concepts

For application purposes, the key concepts of interest to this study are as follows:

Fraudulent e-banking transactions

Fraudulent e-banking transactions are among the most money-spinning types of cybercrime today. According to Van der Meulen (2013, p.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. Although the general assumption is that customers are not liable and that banks refund the financial losses of victims of Internet or e-banking fraud, the banking industry is moving towards customer liability and/or co-reliability. Jansen and Leukfeldt (2015, p.31) emphasize the need to educate customers to avoid fraudulent schemes. According to Andrews and Boyle (2008, p.60), the main inhibiting factors for many forms of transactions which affects customer relations, are that of perceived risk, e-security, trustworthiness, and privacy, especially in Internet banking, which influences customer's perceptions and behavior 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 move towards (co)liability, the focus will be on proactive communication through the website on possible risks of fraudulent transactions and preventative measures. According to Edwin Agwu (2018, p.187), the main concern for banks is a reputational risk which can lead to loss of valued customers, loss of efficient employees, smeared reputation from frauds, customers might shy away to protect their own risk and loss in future cash flows. For the customer, the perceived risk defined by Sathy (1999, p.326) as "the security and reliability of transactions", is the risk of losing money through fraudulent transactions or that personal information might be misused (Drennan, Sullivan Mort & Previte, 2006). It is posited that proactive communication through knowledge sharing can negate potentially these negative risk consequences to enhance customer relationships by taking away the uncertainty for customers and banks by simultaneously making discussions on clarity and constancy obsolete.

Customer (co)liability

Due to the increase in fraudulent 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, the lack of clarity about 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 of which 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 not specified, the 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 anti-software (usually provided by the bank online free of charge). In addition, ignoring the warnings of malware and phishing/vishing/SMishing by clicking on links and responding to emails and mobile communication are serious fraud threats, but the inclusion of more specific terms of use might reduce the lack of clarity and consistency

since banks will then be more transparent about their expectations. (Van der Meulen, 2013).

E-security

Yousafzai, Pallister and Foxall (2003, p.849) defines security as a threat which creates "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse". In the context of e-banking, threats can be made either through network and data transaction attacks or through unauthorized access to the account by means of false or defective authentication. Perceived security then is the customers' perception of the degree of protection against these threats. Studies suggest that the greatest challenge to the e-banking sector will be to gain the trust of customers over the issues of privacy (personal information) and w-security (interception). According to them, financial institutions can build mutually valuable relationships with customers through a trust-based collaboration process. This is particularly true in the case of e-banking where there is a physical separation between the bank and the customer, circumstances are difficult to predict, and the relationships are difficult to monitor. Furthermore, websites can be counterfeited, online identities can be forged and electronic documents can be falsified. Another concern is the lack of adequate regulatory control which leads to the customers' perception that their personal information may be used without their knowledge during or after navigation. Therefore, it is argued that a trusted financial institution will take steps toward the development of institution-based trust associated with the Internet infrastructure and reducing the environmental risk associated with a focal transaction.

Customer relationship building

The Web, specifically the Internet, offers financial institutions the opportunity to build relationships with their customers and stakeholders and can be used to offer diverse information on a variety of information and services, including information on fraud, and to correct misinformation. Despite the growing importance of proactive communication on websites, the research found that websites are limited in terms of communication with customers and employees in fraud prevention, but emphasize the importance to use it as an additional means to and not replace the use of traditional media (Greer & Moreland, 2003). Although no consensus has been reached in the literature on the specific dimensions of sustainable relationships, they are generally considered as a higher order concept encompassing different inter-personal aspects (Larghi et al. 2015, p.18). More recent empirical studies suggest that sustainable customer relationships encompass qualities such as mutual trust, satisfaction, and commitment (Lages, Lages & Lages, 2005, pp.1040-1048) to address perceived risk.
Theoretical framework

The accelerated capacity of e-banking transactions and the Internet can either empower a customer or counteract the threats posed by the increasingly fragmented media landscape. One way to counteract this is to engage with customers through proactive communication and knowledge management by incorporating safety and security messages on the website to warn and reassure customers of prevalent fraudulent transactions. Authors like Gonzàles-Herrero and Smith (2008, p.145) point out that the Internet either acts as a 'trigger' caused by rumors, hacking, copycat websites, web

security breaks and all forms of cyber-terrorism/cyber crooks; or a 'facilitator' as an agent that accelerates messages to provide new knowledge. Consequently, it is argued that the knowledge management theory, one of the most prominent theoretical approaches to study online communication, is one way of facilitating messages for fraud prevention. 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) because it allows for the transformation, sharing and processing of knowledge in four different forms: socialization, externalization, combination, and internalization (Nonaka & Takeuchi, 1995; Barker, 2016). If It is argued that the KM paradigm presents a way to proactively manage and control the messages which are acquired, transferred and assimilated to ensure that knowledge is created, distributed and shared (Nonaka & Takeuchi 1995; Lee et al., 2013).

The starting point of this study is therefore evidenced in the processes of KM as a comprehensive approach to online communication in general, and in this paper particularly with regard to proactive communication for the prevention of fraudulent e-banking transactions. A conceptual framework explains, either graphically or in narrative form, the key constructs, and variables or factors that need to be studied and the presumed interrelationship between them (Miles, Huberman & Saldanha, 2013). For the purpose of this study, a graphical conceptual framework is presented 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. Figure 1 proposes a conceptual theoretical framework for e-banking fraud prevention and (co)liability through proactive communication.

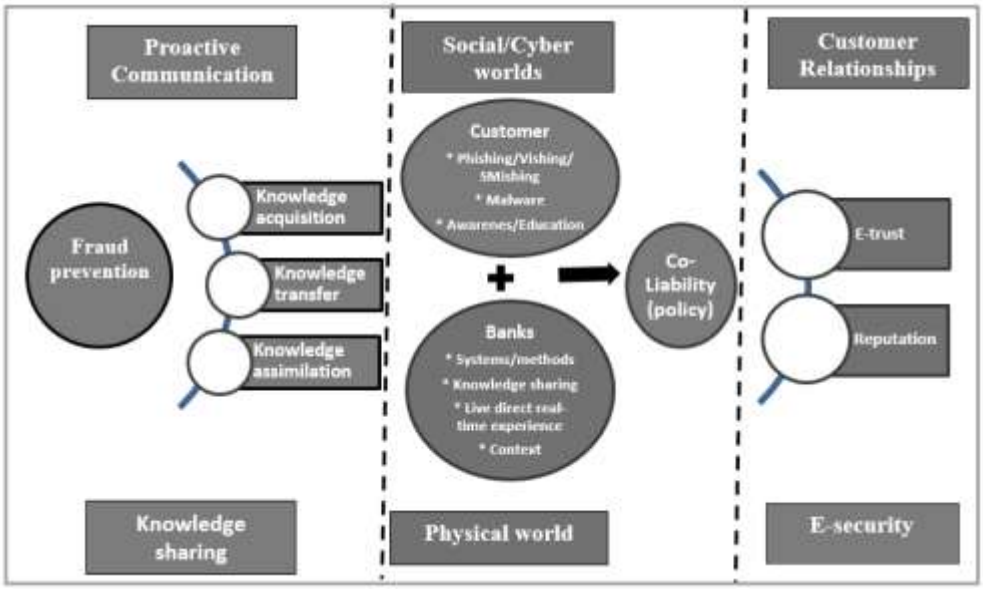

Figure1. Conceptual framework for e-banking fraud prevention and (co)liability through proactive communication

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 based on the discovering of new knowledge. 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 and anti-fraud software 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 of customers to the Security Centre, Online Fraud Updates, media releases, campaigns, general security messages (formal or informal), and detailed methods, practices, and procedures to address it proactively and reactively.

From this theoretical perspective, it is argued that the knowledge management paradigm offers the opportunity to manage and control proactive communication and knowledge sharing (the convenience in assessing information through information and knowledge collection and knowledge donation) as a significant antecedent to address reputational risks and innovation performance. This is done through systems, methods, prompts, direct real-time experiences, etc. to educate, train and create awareness by customers to prevent third-party fraudulent transactions by means of these typologies through a series of messages and links to assure customers of safe and secure online transactions. It is further posited that these typologies should be used consistently and continuously to create awareness on fraudulent e-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/SMishing and malware fraudulent banking transactions and identity theft to prevent these actions. Through constant prompts, customers should be made aware of existing and/or new fraudulent transactions to ensure that the concept of (co)liability becomes a crucial concept in the prevention of fraudulent e-banking transactions. The creation of e-security and e-trust will then lead to sustainable customer relationships to build loyalty and maintain or enhance the reputation of the organization.

Research methodology

This research was conducted through a qualitative research methodology which was conducted in the natural setting of the subject under study and focused on unexplored processes (Babbie, 2007; Chambliss & Schutte, 2006), in other words, the real online

web site available to all users; and entailed a qualitative content analysis of websites on the prevention of fraudulent e-banking transactions and e-security based on the identified and characterized theoretical typologies as indicated in Figure 1. The subject under study was the South African Banking Risk Information Centre (SABRIC) who, on behalf of the banking industry, caution the public on banking crimes through proactive communication and knowledge sharing on their website. SABRIC is a Non-profit Foundation formed by the four major South African banks and has 23 Member Banks to support the banking industry in the combating of crime. SABRIC'S clients are South African banks and major CIT companies with the main business to detect, prevent and reduce organized crime in the banking industry and to co-ordinate inter-bank activities aimed at addressing organized bank-related financial crime, violent crime and cybercrime through the creation of public awareness and deducting the public to protect themselves and acts as a nodal point between the banking industry and others, in respect of issues relating to these crimes.

The measuring instrument employed was therefore qualitative research through a case study-based analysis of the website on fraudulent e-banking transactions of SABRIC selected through a purposive sampling as they present most financial institutions in South Africa, was willing to participate in the research, information of the website was easily accessible, availability of information, the right to use information obtained through data mining, etc. The criteria were derived from a comprehensive literature review and based on the conceptual framework and examined data collected on how SABRIC used their website as one way to manage and control messages in a three-year period (April 2016 to April 2018) before or after incidents of fraudulent e-banking transactions and/or security measures were put in place for the prevention of fraud.

For the purpose of this paper, the four concurrent cyclical flows of activity identified by Miles, Huberman and Salanda (2013) have been used. Firstly, data collection was aimed to investigate the use of proactive online communication to ensure the control and management of fraudulent e-banking transactions. The data gathered was information on preventative measures posted on the SABRIC website during the specified time period and by printing available and accessible pages that were primarily associated with information about the prevention of fraudulent e-banking and/or e-security and safety of online transactions. Secondly, data condensation was used as the process of selecting, focusing, simplifying, abstracting and/or transforming the data that appear in the full body of the selected website information releases in terms of the theoretical criteria and framework (Miles, Huberman & Salanda, 2013). Thirdly, data display was used to organize, compress and assemble the information that allows for the systematic and powerful displays of conclusion drawing. Lastly, drawing and verifying conclusions reflects the interpretation by means of noting patterns, explanations, casual flows, and propositions. These components are interwoven before, during and after data collection to make up the general domain called 'analyses'. The data displayed included all media releases, videos, campaigns and safety measurements on fraudulent e-banking transactions. In order to determine the cumulative number of fraudulent-related messages posted by SABRIC on the website, the researcher conducted a post hoc analysis of the sites' contents. Included in the analyses were additions and deletions of individual company generated messages (for example media releases from the agent or expert). The material printed included fraudulent e-banking transaction specific pages and links to additional information (campaigns, media releases, and videos). Internal validity has been addressed through consistent evaluation of the website addressing the

concepts under investigation. This study also addresses validity through the question of generalization by using the typologies indicated in Figure 1 as generally apparent in knowledge management and proactive communication that can be used in comparative studies in future.

Data analysis

Data was analyzed through an iterative process using coding of data to identify typologies of initial concepts, identify integrative concepts applicable to all the subjects under study and selective coding to reduce it into emergent themes. The researcher also applied the concept 'lurking' as a non-participative observer trying to understand the meaning transferred to the customers through the three components KM and focused only on asynchronous communication (communication with people through a one-to-many approach at different times). During the specified time frame the website monitored resulted in the following main message constructions and links on e-banking fraud prevention as indicated in Table 1.

Table 1. Message construction of e-banking fraud prevention

Proactive communication through KM and sharing	**Message constructions on e-banking fraud prevention**	**Number**
Videos	Cybercriminals are watching you ATM card fraud Carrying cash safely Phishing/vishing Sarah adventures videos	6
Campaigns	We need your help! Small favor, big return (May 2018) Banking Industry launches protection of personal information campaign (May 2017) Keep your money safe this Festive Season (November 2017) SABRIC warns consumers to beware of phishing and malware (June 2016)	4
Media releases	SABRIC Report: Credit card fraud has risen by 1% (April 2018) SABRIC lauds special meeting on cash-in-transit heists (May 2018) Release on card fraud stats 2017 (April 2018) SABRIC & Nelson Mandela University join forces in the fight against cybercrime (March 2018) Money matters matter (March 2018) Ponzi & Pyramid schemes (March 2018) Ngcobo station attack (February 2018) Be careful! Criminals are targeting your Stokvel payout this Festive Season (December 2017) SABRIC: Safe banking over the Festive Season (November 2016) Don't let criminals get their hands on your money – carry cash safely (October 2016) Get rich quickly? (September 2016) SABRIC cautions women to be alert on dating sites and social media platforms (August 2016)	15

Proactive communication through KM and sharing	**Message constructions on e-banking fraud prevention**	**Number**
	Wise Up and Watch Out for Schemes and Scams (July 2016) SABRIC encourages bank consumers to take care of their Cybersecurity (April 2016) You could be sharing too much personal information on social media, SABRIC warns (February 2016)	
Stay Safe (Security center)	Safe banking awareness (links to scams)	18

The video focuses mostly on warnings of cybercrime, ATM card fraud, cash safety and phishing/vishing. The campaigns tried to create awareness on a wide range of fraudulent activities, but also on the importance to protect personal information (identity theft), money safety and phishing and malware practices. From the 15 media releases postings on the website in the monitored period of time, the following types of messages were posted: safe banking (5), cybercrime/security (4), Get-rich schemes (2) and Cash-in-transit heists (2). This is graphically presented in Figure 2.

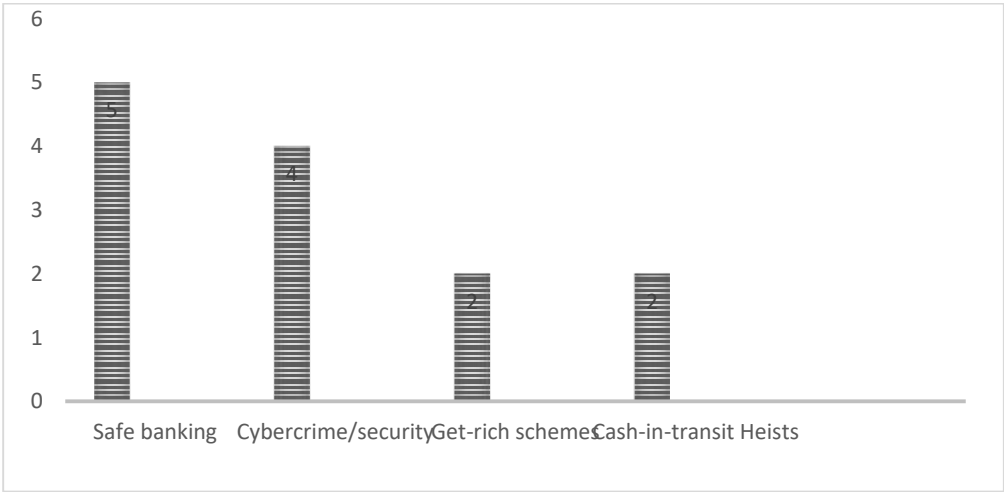

Figure 2. Types of messages in the media releases

From Figure 2 it is clear that prevention measures for safe banking were most prevalent, especially to keep money safe, followed by cybercrime and security where customers are warned about identity theft, the use of social media and dating sites (in other words to keep personal information safe). One example is that of the CEO of SABRIC who said in their latest media release: "Criminals will use these techniques in the hope of tricking recipients into disclosing their personal information on bogus online platforms or on spoofed websites. And all it takes is a few duped individuals to make phishing a profitable business for cybercriminals." SABRIC (2018). In terms of the 'stay safe' website, each of the scams is identified and each of these links provides detailed information on these scams and safety tips on how to prevent fraud.

Table 2 presents the results in terms of the three typologies of knowledge management to ensure that knowledge sharing takes place.

Table 2. Data analysis in terms of the typologies of knowledge management

Typology	Components/ criteria	Variables/results
Knowledge acquisition	Technical (website): data gathering and mining knowledge construction	Wise up. Watch out. (important information on SABRIC) Beware! Skelm is lurking this Festive season. Stay Safe – keep your money safe with these tips Detail information on the banking scams and fraudster statistics All third-party frauds have visual links and each cover a broad spectrum of fraud and safety measures. Messages constructed based on existing data and fraudulent transactions Information not yet prevalent: cryptocurrency fraud and 'SMishing' but has been included in a new media release
Knowledge transfer	Proactive Organizational Communication (messages): create direct real-time interactions sharing of information	Communication through the creation and sharing of detailed messages through direct real-time interactions on the home page Real examples of scams with visual links to give proactive communication messages and information on each of the following scams Card fraud Details of what counterfeit card fraud is What is 'card not present' (CNP) fraud? Lost card fraud Stolen card fraud Account take over fraud Not received issued card Important tips to avoid card fraud ATM What is ATM's (card skimming, swapping cards, ATM shoulder surfing and trapping of cards inside ('Lebanese' loop) Do's Don'ts Tips on protecting your pin Tips for protecting your cash Telephone numbers for reporting ATM-related incidents Internet banking Details on how to using pin and password correctly Make sure you've logged on to your Bank's authentic Internet banking website Is your own PC secure? Tips for using your card safely on the Internet Cell phone banking The safe way to use it as it relies on encrypted SMS messages or secure WAP connections Important notes 419 Scam What is it? Some indications that this could be a 419 scam (if it sounds to be good to be true it is) General trademarks of a 419 scam

Typology	Components/ criteria	Variables/results
		What you should do when you received a 419 scam through letters, emails, fax Changing banking details scam: Definition and discussion of the scam How to prevent becoming a victim of this type of fraud What can you do as a victim? Identity theft What it is What can criminals do with your personal information (assume your identity to access funds, acquire retail or bank accounts, defraud insurance, medical aid and UIF) What is personal information (ID, passport, driver's license, salary advice, municipal bill or other account statements, bank statements) Deposit and refund scams How does it occur? How to protect yourself Money laundering (limited information) Tips to safeguard yourself Carrying cash safely Tips to avoid being a victim of cash robberies for individuals, business, saving clubs and 'stokvels' Phishing What it is(emails) Modus operandi ('spoofed' website) Tips to avoid becoming a victim E-mail hacking Symptoms of a possible compromised email address (spams, unknown emails, etc.) What to do if you suspect your mailbox has been hacked How to prevent email hacking Cybercrime What it is (criminal act) Tips to avoid cyber-crimes Cybersecurity Mobile devices and tablets Software management Connectivity Behavior (tips) Schemes and scams Fraudulent change of bank account details scam (modus operand and awareness tips for consumers) Deposit and refund scams (modus operandi and awareness tips) Dating and romance scams (modus operandi, how victims get defrauded and how to avoid being a victim of online dating scams? (tips) Classified/holiday scams (modus operandi and how to protect yourself) Phishing (modus operandi and awareness tips)

Typology	Components/ criteria	Variables/results
		Telephonic technical support scams (modus operandi and awareness tips) Get rich quick scams (what it is, modus operandi and signs to look out for) Safe banking awareness Mobile banking (prevalent modus operandi through social engineering tactics to trick victims to disclose mobile login details and then conduct a fraudulent SIM swop on this number and safety tips) Internet banking (prevalent modus operandi through phishing using malware to infect the victim's computer and gain sensitive information and passwords and safety tips) Cheques (prevalent modus operandi and safety tips) – see cheque fraud Bank cards (prevalent modus operandi by stealing genuine cheques and dip them into chemicals to removing writing or forge signatures on blank cheques; and tips for cardholders) ATMS (prevalent modus operandi and skimming – mounted, Lebanese loop, card swopping – and safety tips) Money laundering (prevalent modus operandi to avoid access to pay funds into customer's accounts through rewards and tips to safeguard yourself) Festive season scams (prevalent modus operandi to trick customers and safety tips) Vishing What it is (fraudster phone as a bank official or service provider using social engineering skills to manipulate them into disclosing confidential information)) Tips to protect yourself Cheque fraud What it is (cheque interceptions, substitution of genuine issued cheques with fraudulent ones and cheque washing) Look out for … Tips to protect yourself What else to do to keep cheques safe The way you make your cheque payable can protect you How does crossing your cheque protect you? When accepting a cheque make sure … Be cautious when you notice the following on a cheque … Important notes Detailed messages created. Sharing of information through examples of fraudulent emails and direct real-time interactions.
Knowledge assimilation	Human (customer):	The homepage includes warning of fraudulent transactions. Prominent and visual links to all scams

Typology	Components/ criteria	Variables/results
	methods/procedures to link customers informal/formal setting for interaction company practices to address the crisis context	Media and News (press releases) Partners Stay safe (updated details on each fraudulent banking action and latest scams) Contact details General security messages in informal and formal settings. Detailed methods, practices, and procedures provided to customers to ensure security in informal and formal settings. A clear indication of practices to address both proactively and reactively fraudulent online transactions. Clear contextualization of messages

Findings and critical analysis of results

A critical analysis of the results of the proactive communication and knowledge sharing on the website of SABRIC to prevent fraudulent e-banking transactions revealed that the contents of the website closely applied the three typologies of knowledge management identified in the literature review. It is indicative that effective and proactive communication through KM can contribute to manage and control messages for the prevention of fraudulent e-banking transactions to ensure e-trust, loyalty, e-security and a positive reputation of the institution to enhance customer relationships. A summary of the main results in terms of the three typologies are presented as follows:

Knowledge acquisition was evidenced through providing instructing information on the website to customers on how to keep money safe with detailed information on the banking scams and fraudster statistics, visual links to each spectrum of fraud and safety measures, accurate information and messages based on existing data and fraudulent transactions on how to take pro-active action based on data gathering and mining, as well as knowledge construction. Three main types of messages that were obtained through data mining and constructed were noticeable: basic facts about fraudulent e-banking transactions; 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 was verified by the establishment of a 'Stay Safe' security web site and detailed and visual links to cover the broad spectrum and context of fraudulent e-banking transactions.

Knowledge transfer was apparent from the move into creating and adjusting the communication messages once the immediate impact of the fraudulent e-banking transaction wears off by posting various messages and linking customers to websites for direct real-time interactions and by sharing information to ensure them of the save and secure use of online transactions. Examples of possible real-time fraudulent transactions on each link were explained in terms of the modus operandi of criminals, what the scam is, how customers should prevent or address it if it happened, numerous safety tips, etc. to ensure transfer of this knowledge to the customer.

Knowledge assimilation was substantiated through the control and management of the messages in the pre, present and post stages of fraudulent e-banking transactions. This is evidenced in the following: the home page includes warnings to fraudulent

transactions, provide prominent and visual links to all scams, access to media and news (press releases), details on the partners, easy access to the main link to stay safe (updated details on each fraudulent banking action and latest scams), contact details, general security messages in informal and formal settings, detailed methods, practices and procedures provided to customers to ensure security in informal and formal settings, clear indication of practices to address both proactive and reactive fraudulent e-banking transactions with a clear contextualization of messages. These links not only presented methods and procedures to ensure safe e-banking transactions but also provided informal and formal settings for interaction (for example Facebook and Twitter although it was not included this study), stating company practices to address fraud and the context in which it is managed and controlled. This was corroborated through linking of customers to 'Stay Safe', general security messages (formal through media releases or informal through videos), and detailed methods, practices and procedures to address it proactively and if needed, actions to correct actions reactively.

The results of the analysis indicated that the bank definitely complied on all accounts and that most of the criteria of each typology of the knowledge management paradigm were adhered to. Furthermore, it is argued that due to proactive control and management of messages, customers were assured through various means of the safe and secure use of online transactions. Within each of these typologies, the 'expert' initiated messages to react, warn and update customers (proactively and reactively) and included real-time examples and the modus operandi of fraudulent emails, SMS's and scams. The messages were made available quickly and immediately after incidents of fraudulent e-banking transactions became evident (whether through asynchronous media like media releases, links, emails, etc. or synchronous media like Facebook, Twitter, etc.), were factual, and assured customers of security and safety measures applied by the bank throughout. This is in line with the arguments based on the literature review that initial response to fraudulent e-banking transactions should be quick, consistent, open, sympathetic and informative to create awareness and educate customers on e-security and to enhance customer relationship through the three typologies of KM to ensure knowledge sharing. Furthermore, one main link to the 'Stay Safe' was (and still is) evident, visually prominent and easy assessable on the home page. This 'Stay Safe' had 18 main links to each of the fraudulent e-banking scams and fraudster activities with the main aim to 'keep your money safe'. Although the fraudulent e-banking transactions scam (SMishing) was not included on this link, it was mentioned in the link to media and news where they provided the latest press releases on new scams and/or other e-security knowledge and information. For example, the latest press release said: "SABRIC would like to remind bank clients to always be on the lookout for Phishing, Vishing and SMishing scams … to make conscious decision to institute good habits to avoid becoming victims …" (SABRIC, 2018, p.1). Although 'cryptocurrency' (like Bitcoin) was not prevalent either, it could partially be considered under 419 Scam which warns that 'if it sounds to be good to be true it is'. However, due to the vast number of these scams, research is ongoing.

From the above, it is argued that the website messages were organized around the main types of messages identified in Table 1 and if correlated to the typologies in Table 2, it is clear that overlaps exist which means that it is indicative that KM can be used as a theoretical starting point to manage and control the different types of messages to create awareness, educate consumers and share knowledge and information to ensure the prevention of fraudulent e-banking transactions and to enhance e-security and

customer relationships. Generally speaking, the opening website page of SABRIC not only reflected immediate and proactive communication on 'Stay Safe' of the 18 scams, but also provided a direct link to 'Who we are" which includes the staff, vision, values and mission statements highlighting the need to view crime as a shared responsibility and collective priority for customers and public-private partners which can be seen as a first step towards (co)liability; media and news (press releases, campaigns, downloads and videos); a link to 'Our partners' which include the four major banks who initiated this NPF, but also identified the 23 financial partners; and lastly a link to 'Careers' at SABRIC itself which is self-explanatory.

From the knowledge obtained about the indicators of encryption or secure online transaction systems, it can be argued that SABRIC can be seen as having a strong reputation and positive image because of the factual information on e-security and safeguard practices on the website. Messages varied from a general description of the scam and details on how to prevent becoming a statistic Most of the information also featured in the media releases, thus offering multiple connections from dual locations on the website. Furthermore, visual links were established on each security website with detailed information on possible schemes and information on what to do.

From the above, it can be contended that the bank was consistently proactive, used frequent informative messages, included factual information and knowledge sharing messages to assist customers, provided contact details and assured them continuously of the safe and secure use on online transactions. The vision, values, and mission of SABRIC clearly indicate their commitment to crime prevention through proactive communication and the move towards shared responsibility and (co)liability. The use of the 'Stay safe' link is an example of proactive communication and knowledge sharing to reassure and warn customers of fraudulent e-banking transaction and e-security measures through knowledge management as a change agent. Furthermore, they assured customers that if they use the information on these links, there will be safeguards in place which will enhance e-security (e-trust and loyalty) to enhance customer relationships and SABRIC's reputation to act as perceived risk relievers. This could influence perceived risks and e-security positively from a knowledge management paradigm where the agents are regarded as 'experts' in the field who provides reliable and valid knowledge about indicators of encryption or insecure e-banking transactions contributing further to its reputation.

Finally, the most significant attribute was the identification of fraudulent e-banking transactions as a dangerous and real criminal activity and the importance of proactive communication to manage and control the messages in the social, cyber and physical worlds of customers. SABRIC maintained the same basic format of its web site and frequently updated the messages and links. Although the move towards (co)liability is prevalent, it is suggested that a clear policy is needed to apply it consistently and transparently. However, because the bank introduced new messages about the long-lasting effects of fraudulent e-banking transactions and the vast number of new scams, it can be argued that the bank did apply reactive communication in the acutest phase just after the scam became evident (Gonzàlez-Herrero & Smith, 2008, p.151).

Conclusion and implications

By undertaking a KM approach, the study examined proactive communication and knowledge sharing through KM to control messages on fraudulent e-banking transactions. Although this can often result in the construction of opposing viewpoints, it is argued that a way to ameliorate this tendency is to promote recognition of the scams to alleviate concerns about the save and secure use of online transactions

Although the main limitation is that qualitative research through a single case with one institution was conducted, the findings of the study provide insight into the importance of proactive communication on the prevention of e-banking security to ensure continued and positive customer relationships. The next step is to develop a knowledge management strategy for SABRIC to address perceived risks, enhance customer relationships and ensure a positive reputation of the bank. It is recommended that further quantitative research be conducted to obtain a deeper understanding and accounts of the influence of control and management of messages on perceived risk, which was probably pre-eminent by Lee et al. (2013, p.870) who said: "The most influential construct among the KM practices is the knowledge sharing dimension".

References

Agwu, E. (2018). Reputational risk impact of internal frauds on bank customers in Nigeria. *International Journal of Development and Management Review,* 9(1), 175-192. Retrieved from https://ssrn.com/abstract=3120537.

Andrews, L., & Boyle, M.V. (2008). Consumer's accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal,* 11(1), 59-75.

Babbie, E. (2007). *The practice of social research.* 11th Edition. California: Thomson Wadsorth.

Barker, R. (2016). Knowledge management as change agent to ensure the sustainability of emerging knowledge organizations. In S. Moffett and B. Galbraith (eds.), *Proceedings of the 17th European Conference on Knowledge Management* (pp. 45-53), 1-2 September 2016.

Carminati, M., et al. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers and Security*, 53, 175-186.

Chambliss, D.F., & Schutt, R.K. (2006). *Making sense of the social world: methods of investigation.* California: Pine Forge.

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.

Gonzàlez-Herrero, A., & Smith, S. (2008). Crisis communications management on the web: how Internet-based technologies are changing the way public relations professionals handle business crises. *Journal of Contingencies and Crisis Management,* 16(3), 143-153.

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.

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.* Verona, Italy.

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,* 166-170. IARIA.

Lages, C., Lages, C.R., & Lages, L.F. (2005). The RELQUAL scale: a measure of relationship quality in export market ventures. *Journal of Business Research,* 58(8), 1040-1048.

Larghi, S.B., Lemus, M. Moguillansky, M., & Welschinger, N. (2015). Digital and social inequalitities: a qualitative assessment of the impact of the connecting equality program on Argentinean Youth. *Electronic Journal of Information Systems in developing countries,* 69(1), 1-20.

Lee, V., Leong, L., Hew, T., & Ooi, K. (2013). Knowledge management: a key determinant in advancing technological innovation?. *Journal of Knowledge Management,* 17(6), 848-872.

Leite, R.A., et al. (2018). EVA: Visual analytics to identify fraudulent events. *IEEE Transactions on Visualization and Computer Graphics,* 24(1), 330-339.

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

Mhamane, S.S., & Lobo, L.M.R.J. (2012). Internet banking fraud detection using HMM. In Proceedings of the Third international conference on computing, communication and networking technologies, banking (pp.1-4). IEEE. India.

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

Sathy, M. (1999). Adoption of Internet banking by Australian consumers: An empirical investigation. *International Journal of Bank Marketing,* 17(7), 324-5.

Van der Meulen, M.S. (2013). You'ver been warned: consumer liability in Internet banking fraud. *Computer Law & Security Review,* 29(5), 713-718.

Yousafzai, S.Y., Pallister, J.G., & Foxall, G.R. (2003). A proposed model of e-trust for electronic banking. *Techn ovation,* 23(11), 847-860.