


A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions

**Author:**Joel M. Chigada¹ **Affiliation:**

¹Department of Information Systems, Faculty of Economic and Management Sciences, University of the Western Cape, Cape Town, South Africa

Corresponding author:Joel Chigada,
chigadajm@gmail.com**Dates:**

Received: 29 Jan. 2020

Accepted: 03 Aug. 2020

Published: 10 Dec. 2020

How to cite this article:

Chigada, J.M., 2020, 'A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions', *South African Journal of Information Management* 22(1), a1194. <https://doi.org/10.4102/sajim.v22i1.1194>

Copyright:

© 2020. The Authors.
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Read online:

Scan this QR code with your smart phone or mobile device to read online.

Background: This study investigated the end-users' perceptions about the feasibility of deploying biometric authentication systems as intervention solutions to ameliorate card fraud in the South African payment card industry.

Objectives: The objective of the study was to determine if the existing banking technology and telecommunications infrastructure were capable of supporting biometric payment systems.

Method: In this qualitative research, interviews were conducted with 30 sample elements selected from commercial banks, telecommunications companies and other service providers. The sample included individuals working with banking back-end technologies, telecommunications service providers and credit card fraud experts.

Results: The study established that banking technology and telecommunications infrastructure were capable of supporting biometric payment systems. It was revealed that the deployment of biometric systems would mitigate card fraud transactions. However, findings showed that introduction of zero-floor limits led to high traffic volumes, creating congestion on the telecommunications connectivity. Thus, there was a high likelihood that transaction processes would be slow during peak periods.

Conclusion: The implementation of biometric systems required highly skilled information technology personnel to oversee and support these technologies. This was identified as a potential hindrance for banks. The study established that existing banking and telecommunications infrastructure was capable and supported biometric systems. Banks were not keen to invest in an outright biometric environment because of the huge costs that would be incurred in implementing advanced technologies.

Keywords: biometric authentication; card fraud; security protocol; telecommunications; cybersecurity.

Introduction

The credit card industry in South Africa has grown at an enormous rate over the past 20 years. However, this rapid growth has created many new opportunities for cybercrime syndicates. The rapid increase in bank card fraud and cybercrimes is worrisome for financial institutions, merchants, credit card holders and issuers (whole economy). The South African Banking Risk Information Centre (SABRIC) Reports (2016a, 2017a, 2018a, 2019a) state that more than R2.5 billion was lost through card fraud, during the 2016–2019 financial period. There has been an exponential increase in all forms of card fraud transactions. Consequently, debit card fraud is also on the rise despite Europay, MasterCard and Visa (EMV) compliance. This worrisome trend is expected to continue unless there are stringent measures put in place to mitigate it. Grant (2017) states that globally consumers lost more than \$16b in 2016 through identity theft and fraud. Criminals engaging in counterfeit debit and credit card fraud are circumventing EMV (or personal identification number [PIN] or chip technology) by alternating their behaviour to card jamming and swapping at automated teller machines (ATMs) to steal cards or engaging in shoulder surfing to get PINs (SABRIC 2018b). Technology-savvy consumers tend to spot suspicious activities, and are thus able to minimise financial damages. However, criminals are adept at understanding psychology and in most instances use social engineering tactics to exploit human vulnerability leading to the criminals harvesting confidential information like a PIN or password.

Debates have been ensuing between acquirers and issuers on the feasibility of biometric authentication systems (Payment Association of South Africa [PASA] 2019). Chigada (2020) highlights that key issues being debated include the following:

- the ability of the banking technology and telecommunications infrastructure to support biometric payment systems
- the ability of telecommunications infrastructure to handle large transaction volumes in a zero-floor limit environment
- the issuing banks' ability to process voluminous authorisation traffic in a zero-floor limit environment
- merchants' operational costs for increased authorisation requests.

Conducting transactions below the merchant's floor limit perpetuates the fraud cycle as the issuing bank only sees the transaction after an average of 2 days once the settlement process has occurred (SABRIC 2019b). This occurs when the settlement bank is not the same as the issuing bank. MasterCard International Incorporated (2019) states that the use of non-PIN or chip bank cards, high merchant floor limits and the 2-day time delay settlement and clearance processes have significantly contributed to the growth of credit card fraud. With reference to escalating cybercrimes, the Payment Card Industry (PCI) (2019) instructed the PASA to adopt zero-floor limits for all merchants and stop issuance of non-chip or PIN credit cards. Suggestions have been made to adopt more robust security solutions that enhance confidence of the banking clientele, industry and economy as a whole. Chigada and Kyobe (2018) suggest that robust information systems solutions supported by moral principles and coherent cybersecurity legislation might enhance technical and technological security protocols in place.

Despite the evolution of bank cards in relation to conventional value proposition and customer design, technological and aesthetic features, miscreants have devised and use various techniques and technologies to defraud unsuspecting cardholders, acquirers and issuers (VISA 2018). Reports suggest that cybercrime syndicates enlist the services of employees working in financial institutions to gain unauthorised access to information and information systems. Chigada and Kyobe (2018) reveal that deterring bank card fraud and other forms of cybercrimes is an integral and critical component of a national information infrastructure protection strategy that requires concerted efforts from everyone in society. An avalanche of reports shows that the financial services industry is losing a lot of money through bank card fraud. However, there is a dearth of information regarding any research projects that have been undertaken to suggest security solutions to mitigate bank card transactions.

Literature review

South African credit card landscape

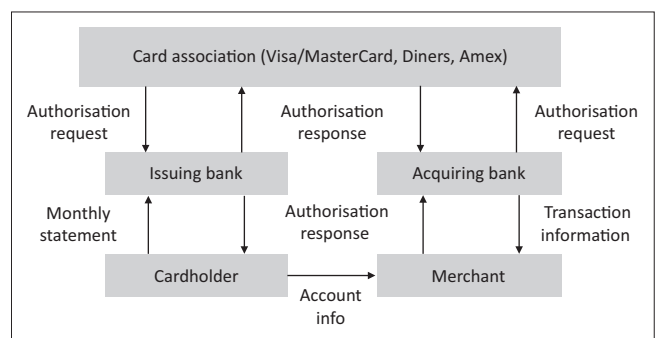
Bank card use in South Africa has increased exponentially since the first credit card was introduced by Nedbank in

1967. Projections are that by the end of 2020, 10 million credit cards will be in use, resulting in a R50b credit card debt. The PCI has indeed become a colossus (Pillay 2016). The bank card is a payment instrument through which purchases can be made utilising the customer's funds and/or credit provided by the issuing bank. Bank card purchases are approved by customers through the signature on the card slip and/or by keying in the PIN on the point of sale (POS) device keypad (PCI 2014). South African bank-issued cards bear the magnetic stripe which is easily compromised by fraudsters and contains sensitive card and cardholder data (card number, expiry date, unique card identifiers) (SABRIC 2017b). Though, chip or PIN technology is fast replacing the conventional bank card, the magnetic stripe is still vital in card transactions in the event that the POS device fails to read the chip or the chip is damaged, in which case the merchant resorts to swiping the card.

How the credit card works

The usage of the bank cards can only be conducted on EMV-certified POS devices which read, validate, verify and communicate with the issuing bank's POS software (Akers et al. 2005). The illustration in Figure 1 summarises the processes involved in card transactions. The current EMV-certified devices on the market include 930 General Packet Radio Services (930 GPRS), 930 Bluetooth (930B), PIN pads, smarts and integrated solutions which are deployed by various merchants who sign service level agreements with the issuing bank that stipulate fees to be paid for all transactions (Nedbank 2018b).

At the pay point, the cashier dips or inserts the chip into the chip reader (it should remain in the device for the full duration of the transaction) or swipes the magnetic stripe on the reader, requests the cardholder to key in the PIN and then waits for authorisation from the issuing bank. If there is sufficient credit and daily limit has not been exceeded, the transaction is approved, or else it is declined. After the successful completion of the transaction, the POS device will issue both a customer and a merchant receipt. Card transactions are approved through the Payment Clearing House (PCH) system operating on a real-time basis, but



Source: Adapted from Akers, D., Golter, J., Lamn, B. & Solt, M., 2005, 'Overview of recent developments in the credit card industry', *FDIC Banking Review* 17(3), 23–35

FIGURE 1: Multi-card issuer model.

clearance and settlement happens in batch mode directly between participating banks (PCI 2016). The acquirer is the institution where a merchant has a bank card account to process transactions and card payments. The acquirer transfers card and other purchase information to a card association which in turn forwards the information to an issuing bank. The acquirer will then credit the merchant for the sales (subject to cleared effects) and send the settlement files to the issuing banks (whose cardholders transacted at the merchant) who in turn will financially reimburse the acquirer and financially account to their respective cardholders' accounts (PCI 2016) (see Figure 1).

Settlement delay

The acquirers engage in commercial relationships with merchants to accept credit cards on the acquirers' POS devices. But before the relationship commences, the acquirer has to be fully satisfied that the merchant has a bona fide business, technology, infrastructure, goods and/or services before signing any contract (PCI 2018). Settlement delays take on average 2 days if the acquirer and issuer are separate entities. The delay is attributed to two separate batch runs, where the acquirer runs one batch to obtain a merchant's sales and create a settlement file for the issuer. On the other hand, the issuer runs a batch file to adjust cardholders' accounts (PASA 2016). The 2-day settlement delay process creates loopholes for fraudsters because it takes time to detect the transaction, especially if issuer and acquirer are two different institutions.

Fraud statistics

SABRIC's Commercial Crime Office, 'Card Fraud Statistics Reports' (2016b, 2017b, 2018b, 2019b) state that Credit Card Fraud has soared in South Africa over the past three years, resulting in the loss of more than R600 million a year. Gross fraud losses (from 2016 to 2019) perpetuated by South African-issued credit cards are illustrated in Table 1. In summary, over the 2016–2019 period, a loss of R201 302 223m was generated through lost or stolen card fraud, R8 502 532m through Not Received Issued (NRI) and R21 598 954m through false application card fraud. Counterfeit card fraud contributed the second most losses amounting to R469 559 032, while account takeover losses amounted to R19 521 784m. The highest fraud losses were committed

through card not present (CNP) to the tune of more than R1.6b. The (SABRIC 2018b) indicates that mobile banking or online applications are experiencing an unprecedented rate of card fraud, resulting in a total loss of R260 007 285m for the 2018–2019 period. More than R2.2b was lost during the 2016–2019 period and it is reported that with the advent of the coronavirus disease of 2019 (COVID-19) global pandemic, cybercrimes are rising exponentially. Cybersecurity experts in South Africa state that there is a sharp increase in cybercrimes such as carding, romance schemes and compromised business emails (Mbopane 2020). Cybercriminals are asking for financial donations on the pretext of procuring medical treatment, personal protective equipment and gear. The (SABRIC 2018b) states that high card and online fraud transactions were mostly recorded in Gauteng, Western Cape and Kwa-Zulu Natal (KZN) and in all three provinces, CNP accounted for the largest card fraud.

Floor limits

A floor limit is a cleared transaction that cannot be matched to a previously approved or partially approved authorisation – or it is transaction submitted without authorisation (VISA 2014). If large volumes of transactions are submitted without authorisation, there is possibility of stressing the back-end processors. Floor limits are generally assigned to the merchant categories with POS devices based on the nature of the products they sell, average ticket value (ATV) of goods and services and the risk propensity of the business. The acquiring bank determines the floor limit based on the merchant category and the current industry standards as governed by the local card association (MasterCard International Incorporated 2019). On the other hand, the issuer funds the risk on the product they issue. The risk-funding is inherent within the interchange that the acquirer pays the issuer for everyday sale. The two types of risks involved are fraud and credit (De Klerk 2015).

Biometric authentication

Ross et al. (2008) define a biometric system as a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. These physiological or behavioural traits include fingerprints, hand geometry, iris, retina, face, hand

TABLE 1: Fraud statistics (2016–2019).

Fraud Type	2016 (R)	2017 (R)	2018 (R)	2019 (R)	Total (R)
Lost and/or stolen cards	15 800 000	25 700 000	81 497 606	78 304 617	201 302 223
Not Received Issued (NRI)	3 100 000	987 000	1 846 630	2 568 902	8502532
False Application	1 900 000	5 500 000	10 294 741	11 304 213	21 598 954
Counterfeit	99 000 000	83 600 000	143 300 000	143 659 032	469 559 032
Account takeover	2 900 000	2 500 000	7 365 437	6 756 347	19 521 784
Card Not Present (CNP)	250 000 000	318 400 000	531 900 000	528 890 000	1.6bn
Mobile Banking fraud	Figures not available	Figures not available	129 002 523	131 004 762	260 007 285
Total losses	372 700 000	436 687 000	873 394 351	902 487 873	2 585 269 224

Source: Adapted from SABRIC Annual Reports (2016a; 2017a; 2018a; 2019a)

vein, facial thermogram, signature or voice to validate or determine an identity. A biometric system may operate either in the verification or identification mode (Biometrics Systems, 2018). In the verification mode, the system validates the person's identity by comparing the captured biometric data with their own biometric template stored in the database (Kumar et al. 2009). Under the identification mode, the system recognises an individual by searching the templates of all users in the database for a match.

When conducting a card transaction, cardholders do not have to carry any bank cards, remember their passwords or secret codes and keep them secured, which can be stolen or lost, thus, exposing the card details to criminals (Chigada & Kyobe 2018). The use of biometrics is gaining popularity in the payment system as a safer and ideal method to combat card fraud and identity theft. In 2009, Walmart and Costco used biometric payment systems that could scan people's fingers to identify and call up payment information. This system was coined 'Pull My Finger...For Payment' and it virtually replaced the use of debit and credit cards at the two chain stores (Kumar et al. 2009). But over the years, with technological advancements, Comstock (2018) states that Amazon and Walmart were granted patents for the use of biometric sensing-systems that detect signs of illnesses and recommend remedies. Walmart's biometric systems for a connected shopping cart handle detect heart rate, palm temperature, grip force and walking speed. The Walmart biometric sensing system is designed to monitor customers running into the store to grab a product, capture a customer's data and relay it back to the central server to check if the customer was or was not satisfied, depending on which the server sends an alert message to a shop assistant to go and help the customer (Comstock 2018).

Rao et al. (2009) state that the use of biometric payment systems is a major milestone in the PCI; even though there are many electronic payment systems, a system is used when users have trust and confidence in it. A system will be accepted if it supports several properties such as atomicity, consistency, isolation and durability, and various other security measures. In 2017, Thales Gemalto introduced the biometric credit card that combines a fingerprint sensor and EMV technology. The card has a design similar to the normal credit card, except that it has a fingerprint sensor which is compatible with all EMV card options, and will include dynamic code verification with an e-link display on the card body in future (Thales 2018).

Initiatives have been taken by the Department of Home Affairs (DHA) in conjunction with SABRIC, who made a joint proposal to the PCI in 2008 (SABRIC 2016a). The project was signed by SABRIC, on behalf of South African Banks and the DHA, to allow banks to conduct online fingerprint verification of their clients' identities, thus allowing banks to have access to the DHA's Home Affairs National Identification System (Hanis). The Hanis database contains South African citizens' identity numbers, fingerprints and photographs (DHA 2010).

In South Africa, Capitec Bank has embraced and uses biometric systems in the credit or loan application system. Capitec Bank introduced the first banking biometric system in 2009 to provide increased security for client transactions and lower banking fees (Capitec Bank 2018). Customers present themselves to the customer sales representative and whilst sitting in front of a web camera, the customer's facial features are captured. The bank's system is linked to the DHA which is the custodian of national identification database, which validates the client's biometric features with the information in its database (identity number, facial and fingerprint information). The system allows immediate verification and instant account access in real time, assuring clients that only they can transact on their accounts. The bank receives a response from DHA and decides the next step in the business transaction (Capitec Bank 2018).

'Hot' card files

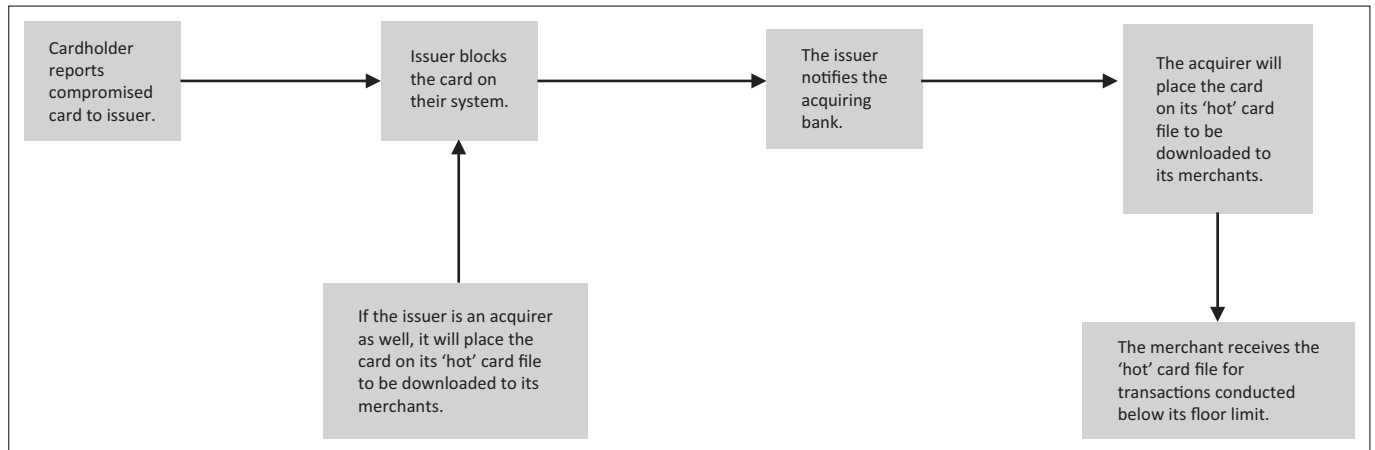
Credit cards can be used fraudulently to transact below the merchant's floor limit because the issuers are at risk as they do not see or acknowledge the transaction(s) until they are settled 2 days later (PCI 2014). In an effort to control the risk, 'hot' card files are created by terminal vendors of POS devices which enable a predetermined number of compromised cards to be stored within the POS host (FastNet 2013). Issuers communicate this information to acquirers who in turn update the POS host with 'hot' card files.

Figure 2 illustrates that the cardholder reports the stolen or compromised credit card to the issuing bank which then blocks the card on its system to avoid any further transactions that can be done. If the issuer is also the acquirer, it places the card on its 'hot' card file to be downloaded to its merchant (Nedbank 2018a). If the issuer is not the acquirer, the issuer notifies the acquirer, who will then place the card on the acquirer's 'hot' card file to be downloaded to its merchants. The merchant receives the 'hot' card file overnight and updates its POS.

The issuing bank has to prioritise the listing of its 'hot' cards. Some of these 'hot' cards may not necessarily be South African-issued cards but might be foreign cards as well. As with the 2-day time delay settlement, there is a 2-day delay when the 'hot' card file is loaded and updated on the merchant's POS if the issuer is not the acquirer as well (PCI 2014). The card can only be loaded on the South African merchant's 'hot' card files for a period not exceeding 60 days, after which it purges. This means that the POS channel cannot be permanently closed and automatically reopens after 60 days. Fraudsters are very much aware of this constraint and use the card for its 4-day life cycle until it is loaded on each merchant's POS (Standard Bank 2018).

Chargebacks

As part of the commercial agreement between the acquirer and merchant, if the merchant transgresses their commercial agreement with the acquirer, the merchant



Source: Nedbank, 2018a, *Card fraud detection training*, Nedbank, Sandowns, Sandton

FIGURE 2: 'Hot' card file process.

may incur a financial loss attributed to the disputed sale (Standard Bank 2018). The issuer also has financial recourse to the acquirer in cases where the merchant did not follow the prescribed association rules. This financial recourse to the acquirer or merchant is called a chargeback. For instance, if a merchant picks up that the credit card is a 'hot' card and still decides to process the transaction, this is an outright violation of association rules, hence a chargeback. The merchant will have no recourse to this transaction (Standard Bank 2018).

Methodology

An interpretivist research paradigm was adopted to elicit the views of subjects who worked with the information communication infrastructure and platforms discussed in this article. Creswell (2014) states that paradigms in human and social sciences help human beings understand a phenomenon and advance assumptions about the social world. Literature suggests that paradigms enable us to understand how science should be conducted and what constitutes legitimate problems (Kuhn 1970). The author was keen to hear the personal voice, accept qualitative words and understand personal experiences (Ngulube 2014). An exploratory research design was adopted, and it acted as the framework of inquiry to complete this study. The exploratory research design helped to explain this study because there was a high level of uncertainty and ignorance about the subject. The problem under investigation was not well researched in the South African PCI, therefore, it was not well understood (Saunders, Lewis & Thornhill 2016). The aim was to identify boundaries of the environment in which the problems, opportunities or situations of interest were likely to reside, while identifying salient variables that might be found and be of relevance to the research project (Romm & Ngulube 2014).

Qualitative research is typically used to answer questions about the complex nature of phenomena, often with the purpose of describing and understanding the phenomena from the participant's perception, perspective and understanding of a particular situation (Leedy & Omrod

2014). Tesch (1994:147) opines that in qualitative research, the researcher and participants work together to arrive at the heart of the matter. The nature of this research included a strong component of exploration and interpretation of events and situations, resulting in the conducting of face-to-face and focus group interviews. Inductive reasoning was used in some cases based on interviews and observed events. Saunders et al. (2016) concur with Leedy and Omrod (2014) in that qualitative research is also used to answer questions about relationships amongst measured variables with the purpose of explaining, predicting and controlling phenomena. During data collection, the researcher suspended any preconceived notions or personal experiences that could unduly influence the research as participants could say anything any time.

Target population

Saunders et al. (2019) define population as the group of elements or objects of interest to the researcher from whom data is collected to address a management problem. The population comprised systems engineers, telecommunications engineers, card fraud experts, business systems analysts, network engineers, strategy specialists, biometric authentication systems experts and Visa and MasterCard International consultants. Sample elements were from Capitec, Nedbank, First National Bank, Absa, Standard Bank and telecommunication services providers. A total of 120 experts made the population for this study. However, in this qualitative research project, 10 participants were selected using non-probability purposive sampling and convenience sampling techniques to partake in the face-to-face interviews. Another 20 participants were selected using probability random sampling for the study.

Creswell (2014), Ngulube (2014) and Romm and Ngulube (2014) state that face-to-face interviews are time consuming. Therefore, in qualitative research between 6 and 12 participants suffice for face-to-face interviews, while between 6 and 20 participants are ideal for a focus group. Bryman (2010) differs with the authors above and recommends

between 8 and 15 participants for face-to-face interviews. In this study, the suggestions by Creswell (2014) and Romm and Ngulube (2014) were adopted. Kumar (2005:179) states that the use of purposive sampling is determined by 'the judgement of the researcher as to who can provide the best information to achieve the objectives of the study'. This assertion by Kumar (2005) is corroborated by Leedy and Omrod (2014) who state that the use of purposive sampling depends on the researcher's judgement as to who to include or exclude from a sample. The subjects selected for this study possessed the technical knowledge of how banking technologies and telecommunications infrastructure work. Therefore, the data required to address the problem resided in the selected subjects.

Data collection

Interviews are an important part of any research project as they provide the opportunity for the researcher to investigate further, to solve problems and to gather data which could not have been obtained in other ways (Cunningham 1993:93). Saunders et al. (2019) state that an interview is essentially a qualitative data collection technique where the interviewer directs the interaction and inquiry in a very structured or unstructured format. An interview guide was designed in line with research objectives, whose main aim was addressing the banking and telecommunications infrastructure, ability to sustain and process high volumes of transactions in a zero-floor limit environment and the costs incurred by merchants. The interview guide comprised five sections. *Section A* included demographic variables such as age, position (or title), years of experience, gender and race. This information was paramount to mitigate any bias that could have arisen in the event of exclusivity occurring. *Section B* focused on the ability of banking technology and telecommunications infrastructure to support biometric authentication systems. In *Section C*, the study sought to determine the ability of telecommunications infrastructure to sustain zero-floor limit transactions arising from high request volumes. In *Section D*, the aim was to establish the issuing banks' ability to process high transaction volumes in a zero-floor limit environment. The last section (*Section E*) sought to establish the additional costs incurred by merchants for telephone services when requesting authorisation. All questions were open-ended, creating opportunities for subjects to explain viewpoints in their own words (Stangor 2011). Secondary data, in the form of industry reports, were provided by SABRIC, PASA and the Internet.

Ethical consideration

The study received ethical clearance from the Faculty of Commerce, University of Cape Town (REF: REC2018/001/005).

Discussion of findings

Thematic data analysis (TDA) was performed through the lens of Atlas Ti. v6. Braun and Clarke (2012a) posit that TDA

helps to convert qualitative data into meaningful information because the researcher is able to extract rich sets of data and describe events as they occur in a natural setting. From a total of 30 participants, 13 (43%) respondents were female, while the majority (57%) of the respondents were males.

Banking technology and telecommunications infrastructure's ability to support biometrics

The study established that most of the commercial banks' transaction manager (Base 24 and Base 26) systems were scalable and could incorporate biometrics and Alieno authentication systems. The configuration of the Transaction Manager Base 24, an enterprise resource planning (ERP) system concurs with the views raised during the interviews. The consensus from respondents was that:

'The banking ERP systems were scalable and could be integrated with other platforms.' (PB02, Systems engineer, 2019)

'The challenge confronting all banks is the cost of implementing new and managing multiple technologies. The cost entails hiring SAP consultants, IT professionals and acquisition of software and hardware.' (PB01, Focus group, 2019)

'It is important to acquire and implement technologies aligned to organisational strategy, to generate customer and shareholder value.' (PB04, IT Strategist, 2019)

The BankServ Annual Report (2011) highlights that as part of security measures, banking platforms should be designed to incorporate and integrate with other cybersecurity and information systems especially in the dispensation of rising information, information systems and cyberattacks and threats. Chigada and Kyobe (2018) concur with the assertions in the BankServ Report (2011) in that various interventions including legislation, technical and technological systems and moral standards play an important role in combating cybercrimes. Systems Applications and Products (SAP) (2015) argues that most of its ERP systems in the market are scalable and can incorporate other systems; however, a huge financial investment would be required to develop an integrated and complex architecture. The report by SAP (2015) disputes the notion that has been widely spread that current banking technologies cannot integrate biometric systems; however, it is the cost element that impedes integration of such systems.

Telecommunications infrastructure's ability to sustain high transaction volumes

Interviews were conducted with participants providing telecommunications services such as GPRS for POS devices, telephone lines, asymmetric digital subscriber line (ADSL) and other services. However, the telecommunications services providers indicated that merchants should be prepared for high telephone service costs to ensure that best equipment was installed to mitigate time-out problems which might persist. The findings showed that the scarcity of information technology and telecommunications engineering skills was a major impediment in the country. That response was least expected in the study, but it was

paramount because it confirmed one challenge confronting South Africa – skills shortage in the sciences disciplines (StatsSA 2018). It was revealed that South Africa's telecommunications infrastructure was one of the most stable, reliable in the region, therefore, had the capacity to sustain large transaction volumes (Telkom SA 2014). The most basic idea about telecommunications is that the electronic signals are sent on the network as either analogue or digital depending on the type of the network. Most of the POS smart devices used by merchants in South Africa, use the telephone network (analogue) to process card transactions.

The volume of data that is transmitted per unit of time constitutes the speed of transmission. Gillwald, Moyo and Stork (2012) point out that it is important to consider the speed of transmission between the merchant's POS device and response from the bank. The bandwidth or capacity to transmit large volumes should be used as a determining factor on the ability of telecommunications infrastructure. The Secure Socket Layer (SSL) 128 bit is a good example of leased and secure line for data transmission. These lines are mainly used to transmit data where high security levels are envisaged (Gillwald et al. 2012). Therefore, the telecommunications infrastructure was capable of sustaining high transaction volumes. Some of the responses from the study that support the above narrative were:

'South Africa's telecommunications technology and infrastructure is of global standards. It is benchmarked against that of Germany, Australia, United Kingdom, therefore, it can sustain high transaction volumes.' (PB01, Telecoms engineer, 2019)

'Our telecommunications infrastructure is capable to handle large transactions. It can support biometrics and zero-floor limits, however, banks should reconfigure their models and architectures. Some amount of redesigning is required where IT experts and engineers are required.' (PB05, Telecoms service provider, 2019)

The narratives above also reveal that the telecommunications infrastructure was suitable for supporting and carrying biometric authentication requests. However, banks were required to redesign their existing systems. The study revealed that the DHA, Capitec Bank and other institutions in South Africa were at the forefront of using biometrics, using the same telecommunications configurations. Capitec Bank introduced the first banking biometric system in 2009 to provide increased security for client transactions (Capitec Bank 2010). The system allows immediate verification and instant account access in real time, assuring clients that only they can transact on their accounts.

The ability of banks to sustain and process large transactions is attributable to redesigning or configuration of front-end processors and hardware (Blue Label Data Solutions 2017). Evidence from the study showed that in 12 bankable hours, millions of banking sessions are processed by banks; therefore, banks have the capability to process huge transaction volumes that arise in zero-floor limit environment.

To augment the argument, Capitec Bank introduced biometrics with the aim of increasing security for client transactions and lower banking fees (Capitec Bank 2018). The system allows immediate verification and instant account access in real time, assuring clients that only they can transact on their accounts.

Issuing banks' ability to process huge authorisation requests

It was established that issuing banks' front-end processors had the capacity to process huge authorisation requests. During a 2-h observation at one of the research sites, more than 2 million banking sessions (authorisation requests) were processed. At that load level, the banking platforms were processing more than eight times as many banking sessions per hour. De Klerk (2015) states that the unused capacity of bank's front-end processors is used to accommodate intra-day spikes. Literature points out that banks can process millions of banking sessions in a 24-bankable-hour period (BankServ 2016). Furthermore, it was revealed that setting merchant floor limits to zero was welcome despite huge transaction requests processed; however, merchants would be expected to pay high telephone services costs.

The study revealed that there was need to redesign architecture of front-end processors and increase their capacity to cater for huge transactions (Blue Label Data Solutions 2017). This would envisage a complete overhaul of the hardware and software to ensure there is smooth processing of transactions. In the absence of increased CPU capacity, time-out problems will persist and this will affect merchants and cardholders. It was also revealed that most banks used the Transaction Manager Base 24, an ERP scalable system that supports Alieno and biometric authentication. These revelations are supported by the following response:

'Banks can handle large transaction volumes. However, there can be a challenge if there is an influx of zero floor limits. The system can be clogged and slowed down. This is also good because it allows the bank to conduct due diligences on each transaction before authorisation. The downside is that merchants become angry at the speed of their POS devices. At times merchants unplug and plug telephone cables to the POS.' (PB01, Focus group, 2019)

High operational costs incurred for telephone services when requesting authorisation

With reference to the discussions relating to processing of huge transaction requests, the study also revealed that the introduction of zero-floor limits is a welcome strategy to mitigate credit card fraud. However, the downside was that merchants were expected to pay more for telephone services (De Klerk 2015). High costs would be incurred when the merchant calls the acquirer, who then dials the issuer through BankServ for authorisation and back to the merchant with a response. Huge transaction volumes are involved in such cases, resulting in merchants paying higher fees. If biometrics are involved, merchant costs are

reduced because no dialups are required to authenticate the transaction. Some responses that demonstrated the high telephone costs were:

'Merchants pay high transaction costs for large transaction volumes because they consume high bandwidth. In addition, duration for each transaction is prolonged.' (PB05, Telecom service provider, 2019)

'In the event of deploying biometrics systems, it would mean that banks will incur reconfiguration/redesigning costs, which are in turn passed on to merchants. Overall, the switch to biometrics will be costly because merchants are already paying high telephone costs.' (PB08, Business analyst, 2019)

Telkom SA (2017) acknowledges that South African telecommunication services are some of the most expensive services in the world due to high interconnection rates. The Independent Communications Authority of South Africa (ICASA) (2020) states that major cellular operators – Vodacom, MTN, Virgin Mobile and Cell C – have engaged in discussions to reduce call and data rates. Merchants using telecommunication services from cellular firms are affected by a fluctuation in off-peak and peak internet call costs. Both banks and merchants carry the costs, but the greater part of the costs is carried by merchants (Nedbank 2018a).

Setting merchant floor limits to zero is a welcome initiative for the PCI, however, both telecommunication service providers and merchants should have stable and reliable telecommunications systems in place to mitigate time-out problems which are synonymous in high transaction environments (Chigada 2020).

Conclusion

This was a pioneering academic study that showed the importance of curbing and mitigating credit card fraud. The objective of the study was to determine the feasibility of deploying biometric authentication and zero-floor limits as a way of eradicating card fraud. In addition, the study sought to establish if the existing banking technology and telecommunications infrastructure were capable of supporting biometric payment systems. The objectives of the study were achieved by gathering relevant data from a diverse spectrum of individuals working with banking and telecommunications infrastructure. Their experiences, expertise and knowledge addressed the problem at hand. Some responses were cited verbatim, demonstrating participants' experiences with different systems and challenges. The study confirmed that integration of biometric authentication systems was partially feasible. Bank back-end and telecommunications infrastructure were capable of handling large transaction volumes. However, integration of biometric authentication will increase transaction costs and merchants are not keen on accepting these extra costs.

The research study was exposed to methodological and research limitations. The sample size was not large enough to be representative of a large population. This was attributable

to the qualitative research method used. A large sample size would be achieved if a quantitative or mixed method was used. The study suffered as a result of lack of prior research on the topic in the South African context, which would have laid the foundation for understanding of the discourse investigated. This study depended on having access to people, organisations and data. The researcher could not access some of the resources required to accomplish the study. For further research, an area of interest would be interrogating employees' ethical behaviour in information sharing. This might uncover pertinent issues that exacerbate card fraud and identify theft transactions. Researchers might also look at the effects of COVID-19 on card fraud and online transactions amidst lockdown.

Acknowledgements

This article would not have been successful had it not been for a number of people who contributed to it. I would like to thank all participants for participating in the face-to-face interviews. Thank you all for the insights shared during the period of this study.

Competing interests

The author has declared that no competing interests exist.

Author's contributions

The author developed the article and confirms he is the sole author.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any affiliated agency of the author.

References

- Akers, D., Golter, J., Lamn, B. & Solt, M., 2005, 'Overview of recent developments in the credit card industry', *FDIC Banking Review* 17(3), 23–35.
- BankServAfrica, 2011, *Card fraud and identity theft on the increase: Challenges for the payment card industry*, Selby, Johannesburg.
- BankServAfrica, 2016, *Africa reports big jump in digital and card fraud*, Blue Label Data Solutions, Annual Report, Sandton, Johannesburg.
- Biometric Systems, 2018, *Biometrics in retail banking*, viewed 10 July 2019, from <https://www.blts.co.za/biometricssystem/southafrica>.
- Blue Label Data Solutions, 2017, *Data Explosion and data governance in South Africa*, viewed 18 December 2019, from <https://bllds.co.za/>
- Braun, V. & Clarke, V., 2012a, 'Thematic analysis', in *Encyclopedia of quality of life and well-being research*, pp. 6625–6628, Springer, Dordrecht, the Netherlands.

- Braun, V. & Clarke, V., 2012b, 'Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning', *The Psychologist* 13(2), 12–23.
- Capitec Bank, 2010, *Transforming the banking sector: Challenging the status quo*, Stellenbosch, Cape Town.
- Capitec Bank, 2018, *Revolutionary paperless identification system*, Stellenbosch, Cape Town.
- Capitec Bank South Africa, 2018, *Biometrics authentication*, viewed 17 June 2019, from <https://www.capitecbank.co.za/biometricsproject/htm>.
- Chigada, J., 2020, 'Towards an aligned national cybersecurity framework for South Africa', Unpublished PhD dissertation, University of Cape Town, Cape Town.
- Chigada, J. & Kyobe, M., 2018, 'Evaluating factors contributing to Misalignment of the South African National cybersecurity policy framework', in *Conference Proceedings for the Conf-IRM 2018*, Ningbo, China, June 04-06, 2018.
- Comstock, J., 2018, *Walmart and Amazon patents could take biometric monitoring to new level*, viewed 26 May 2020, from <https://www.mobihealthnews.com>.
- Creswell, J.W., 2014, *Research Design: Qualitative, quantitative and mixed methods*, 4th edn., V. Knight (ed.), Sage, Lincoln.
- Cunningham, J.B., 1993, *Action research and organisational development*, Praeger, London.
- De Klerk, H., 2015, 'Card operations & processing manager', *Personal Interview*, 13 October 2010, Braampark, Braamfontein.
- FastNet, 2013, *Concerns around bank biometrics systems*, ITWEB, Midrand.
- Gillwald, A., Moyo, M. & Stork, C., 2012, *Understanding what is happening in ICT in South Africa: Evidence for ICT Policy Action*, Policy paper, 2 of 2012, Research ICT Africa, Cape Town.
- Grant, K.B., 2017, *Identity theft, fraud cost consumers more than \$16 billion*, *CNBC News*, viewed 10 November 2019, from <http://www.cnbc.com>.
- Independent Communications Authority of South Africa (ICASA), 2020, *Bi-annual report: Analysis of standard prepaid data tariffs and data bundles*, ICASA, Pretoria.
- Kuhn, T.S., 1970, *The structure of scientific revolutions*, 2nd edn., University of Chicago Press, Chicago, IL.
- Kumar, A., Hyun-Joo, L. & Youn-Kyung, K., 2009, 'Indian consumers' purchase intention toward a United States versus local brand', *Journal of Business Research* 62(5), 521–527. <https://doi.org/10.1016/j.jbusres.2008.06.018>
- Kumar, D. & Ryu, Y., 2009, 'A brief introduction of biometrics and fingerprint payment technology', *International Journal of Advanced Science and Technology* 4, 25–38. <https://doi.org/10.1109/FGCNS.2008.11>
- Kumar, R., 2005, *Research methodology: A step-by-step guide for beginners*, 1st edn., Sage, New Delhi.
- Leedy, P.D. & Omrod, J.E., 2014, *Practical research, planning and design*, 12th edn., Pearson Education International, Hoboken, NJ.
- MasterCard International Incorporated, 2019, *Annual reports on payment solutions*, Purchase, New York, NY.
- Mbopane, L., 2020, *SA to lose billions of Rands from Cybercrimes during COVID-19*, viewed 10 July 2020, from: <https://safetyandsecurityafrica.com/sa-to-lose-billions-of-rands-from-cybercrimes-during-covid-19-experts-warn/>
- Nedbank, 2018a, *Card fraud detection training*, Nedbank, Sandowns, Sandton.
- Nedbank, 2018b, *Steps when conducting a chip/pin credit card transaction*, viewed 02 December 2019, from <https://www.nedlink.co.za/pin/chiptechnology>.
- Ngulube, P., 2014, *Research methods in information science*, University of South Africa, Pretoria.
- Payment Association of South Africa, 2016, *Annual report, Payments study tour report*, Reserve Bank of South Africa, Pretoria.
- Payment Association of South Africa, 2019, *Annual report, The National payment system framework and strategy*, Reserve Bank of South Africa, Pretoria.
- Payment Card Industry, 2014, *Data security standard*, Payment card industry compliance workshop, Johannesburg.
- Payment Card Industry, 2018, *Information security standards*, Payment card industry compliance workshop, Johannesburg.
- Payment Card Industry, 2019, *Compliance challenges*, Payment card industry compliance workshop, Johannesburg.
- Pillay, K., 2016, *Card fraud stats 2016*, SABRIC, Cape Town.
- Rao, B.T., Vedavalli, E., Aditya, K. & Bindu, D.R.S., 2009, 'Major milestone in the payment card industry', *International Journal of Computer Science and Network Security* 9(9), 123–133.
- Romm, N. & Ngulube, P., 2014, 'Mixed methods research', in E.R. Mathipa & M.T. Gumbo (eds.), *Addressing research challenges: Making headway for emerging researchers*, Mosala-Masedi, Sandton.
- Ross, A., Murdoch, S.J., Drimer, S. & Bond, M., 2008, 'Chip and PIN is broken', in *IEEE Symposium on Security and Privacy*, IEEE, Berkeley/Oakland, CA.
- Saunders, M., Lewis, P. & Thornhill, A., 2016, *Research methods for business students*, 10th edn., Prentice Hall, Harlow.
- Saunders, M., Lewis, P., Thornhill, A. & Bristow, A., 2019, *Research methods for business students*, 12th edn., Pearson Publishers, Harlow, UK, viewed 03 October 2019, from <https://www.researchgate.net/publication/330760964>.
- South African Banking Risk Information Centre (SABRIC), 2016a, *Annual report*, SABRIC, Midrand, Johannesburg.
- South African Banking Risk Information Centre (SABRIC), 2016b, *Release of Card Fraud Stats 2016*, viewed 10 December 2019, from <http://www.sabric.co.za>.
- South African Banking Risk Information Centre (SABRIC), 2017a, *Annual report*, SABRIC, Midrand, Johannesburg.
- South African Banking Risk Information Centre (SABRIC), 2017b, *Card Fraud Booklet 2017*, viewed 10 December 2019, from <http://www.sabric.co.za>.
- South African Banking Risk Information Centre (SABRIC), 2018a, *Annual report*, SABRIC, Midrand, Johannesburg.
- South African Banking Risk Information Centre (SABRIC), 2018b, *Card Fraud Booklet 2018*, viewed 12 December 2019, from <http://www.sabric.co.za>.
- South African Banking Risk Information Centre (SABRIC), 2019a, *Annual report*, SABRIC, Midrand, Johannesburg.
- South African Banking Risk Information Centre (SABRIC), 2019b, *Crime Statistics 2019*, viewed 10 December 2019, from <http://www.sabric.co.za>.
- Standard Bank, 2018, *Chargebacks training*, Standard Bank, Johannesburg.
- Stangor, C., 2011, *Research methods for the behavioural sciences*, 4th edn., Wadsworth, Cengage Learning, Belmont, CA.
- Systems Application Products, 2015, *Annual report*, viewed 12 May 2018, from http://www.annualreports.com_comany_sap-ag.
- Thales, 2018, 'Biometrics payment card (fingerprint authentication)', *Discover the new biometric card from Gemalto*, viewed 02 January 2020, from <https://www.thalesgroup.com-cards>.
- Tesch, R., 1994, 'The contribution of a qualitative method: Phenomenological research', in M. Langenbach, C. Vaughn & L. Aagaard (eds.), *An Introduction to Educational Research*, Allyn and Bacon, Needham Heights, MA.
- Telkom SA, 2014, *Group annual results for the year ended 31 March 2014*, Telkom SA, Centurion.
- Telkom SA, 2017, *Integrated Report for the year ended 31 March 2017*, Telkom SA, Centurion.
- Unisys, n.d., *Fingerprint authentication*, viewed 18 May 2019, from https://www.unisys.com/biometrics_fingerprints.
- Unisys, 2019, *Consumers' views and perceptions on biometrics payments*, viewed 01 December 2019, from <https://www.unisys.com/survey/consumerviews/biometrics>.
- VISA, 2014, *Financial inclusion and literacy*, viewed 13 March 2019, from <http://www.visa.co.za/html/>.
- VISA, 2018, *Annual report: Card Fraud Soaring*, viewed 31 October 2019, from <https://www.visa.com/html>.