**Industrial Attachment Log Book**

**Name Priveledge Tatenda**

**Surname Mtemashinga**

**Registration Number B1747335**

**Program Computer Science**

**University Bindura University**

**Place of Attachment Steward Bank**

**Department Information Services**

**Supervisor Mr V Gumbo**

**2. Company Background and History**

Steward Bank was launched in July 2013 following Econet Wireless Zimbabwe’s acquisition of TN Bank, a subsidiary of TN Holdings Limited (now known as Lifestyle Holdings). Following its launch, the Bank has since positioned itself as a mass-bank, focused on providing banking solutions through the use of technology.

Steward Bank is the first bank in the country to have convergence with telecommunications and together with its technology focus the bank is set to change the way Zimbabweans view banking.

The future prospects of Steward Bank are very promising, with a total capital base which stood at $75 million on 28 Feb 2013, which is well in excess of the Reserve Bank of Zimbabwe’s requirement of $50 million by June 2013. In addition to this the liquidity ratio has seen remarkable improvement from 5% at 31 December 2011 to 25% at 28 February 2013. In terms of the external credit rating, Steward Bank’s GCR Company rating has improved from a BB rating in October 2010 to BB+ in October 2012. All very positive indicators of a bright and prosperous future for the bank and its clients.

Products produced are as follows

Batsi the Bot. It is a Bot that will increase responses to customer queries by seconds compared to waiting for close to an hour to get a response from a human-assistant. Batsi is a major highlight of the exhibition because it underlies Square 2.0 and social media banking. The Bot will also be used to access banking services like requesting mini statements, bank balance enquiries, sending and receiving money etc. Batsi’s assistance will change the landscape of conversational commerce in Zimbabwe because many banks haven’t adopted this technology hence Steward bank initiative could cause ripple effects in terms of similar adoption of Bots by other banks.

Sosholoza is a revolutionary banking product we have introduced on the WhatsApp platform. Sosholoza offers Zimbabweans a universal and simple of speedily transferring funds from bank account to any wallet, from a mobile wallet to any bank. Sosholoza is really simple as there is no registration necessary. All you have to do is save 0777 222 333 to your contacts and send a message that says, “Hi”. Our bot, Batsi, will lead you through some short and easy steps and you are good to go. Banking on this platform is as easy as it is to send a message on WhatsApp.

**2.1 Mission Statement**

We provide customized innovative world class products and services through convenient channels, technologies and dedicated employees.

**2.2 Vision Statement**

To become one of the biggest banks in Zimbabwe by customers and balance sheet size by 2019

**2.3 Value Statements**

**HEPII**

**Hunhu/Ubuntu**

We respect all mankind and take another person’s challenges as our own. We are not individuals…we are a community.

**Excellence**

Our standard of service surpasses the ordinary, perfection is unattainable however we strive for excellence in every sphere of operation, continuously learning and improving on service quality.

**Professionalism**

We are experts and have specialized knowledge in our area of operation, **performing our work with dedication.**

**Innovation**

We will innovate and continuously develop life changing products and services that create value for all our customers.

**Integrity**

As a bank our actions, methods, principles, expectations, and outcomes are ethical, honorable, truthful and accurate.

**2.4 Core Business**

It is a commercial bank in Zimbabwe which provides services such as accepting deposits, making business loans, and offering basic investment products that is operated as a business for profit. Its main aim is to make banking easier and able to reach from all corners

**4.1 Attachment Experience**

**14-16 August 2019**

**DESCRIPTION OF WORK DONE**

* Introduced to the IT stuff.
* Reading and understanding of the ICT documents including a security policy.
* Asked questions by the management on the policies which I had read in order to show my understanding of it before signing access forms, as a sign of agreeing to conform to the policies

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* To interact with the work flow and the quickly adapt with the working environment.
* I leant the required information needed in the organization and the security responsibility on use of the organizational resources such as the network and the personal computer for the company.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**19-23 August 2019**

DESCRIPTION OF WORK DONE

* Induction
* Channels monitoring

SKILLS APPLIED/ NEW SKILLS LEARNT

* In induction I learned about the products of the company that is, what the company produces for it to survive on the market. The company has online products which are Sosholoza, kashagi and many others. I leant how they market their products to their customers and risk department, what is does and what value it adds to the company.
* I leant about the process in which the channel moves from the point of sale going through the postilion which is a payment switch which is used to determine where the card belongs to. We used Real Time Monitoring which goes to the Postilion payment switch server. The real time monitoring will be showing the transaction manager which manages all transactions that passes through Postilion. It also contain the TermApp which manages all POS that is if it is down, no transactions will go through which comes through the Point of Sale and lastly there is eSocket server which is manages all services that are done through the \*236# which is for opening Isave accounts, iStudent account and Dura FCA, activation of the cards that belongs to the accounts mentioned above by filing in the card details that is, the card number, and the account number in which the card is to be linked with.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**26-30 August 2019**

**DESCRIPTION OF WORK DONE**

* Employee registration on the ZSS portal
* Accessing the ZSS portal
* Channels monitoring

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* ZSS portal is used for accessing transactions on all channels be it transactions from POS machine, wallet to bank and bank to wallet to mention a few. The ZSS portal gives us access to all accounts that are in ZSS that is, revealing balances if a customer have an unsuccessful payment which might have deducted the customer account so as to reverse the transaction through the operation team. On giving access to employees, a user has to sign a access form specifying what the user needs and the document is to be signed by the line manager and any other manager for authorization. The security department will the sign to give us permission to give the user credentials that is, username and password, to access the portal.
* I leant about the process in which the channel moves from the point of sale going through the Postilion which is a payment switch which is used to determine where the card belongs to. It uses the post card to determine the details of the card that is the name, the card number and the account number. If the card belongs to the Steward bank, it then proceeded to either the ZSS or the T24 for the transaction to succeed and if the card belongs to other banks it then goes through ZIMSWITCH which will determine the card issuer through the Bank Identification Numbers (BINs).

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**02-06 September 2019**

**DESCRIPTION OF WORK DONE**

* Employee registration on the Steward Bank portal
* Accessing the Steward Bank portal
* Channels monitoring

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* Steward bank portal is used for accessing transactions on all channels be it transactions from POS machine, wallet to bank and bank to wallet to mention a few. The SB portal is also used for normalization that is, checking if the transactions are up-to-date. All transaction from the core banking that is, T24, are displayed on this portal. It is also used to check if a given account was registered in the banking system or not. We were able to see accounts from the T24 and Isave accounts.
* I leant about the postbridge which manages all services that are managed by the Steward bank such as StewardbankPOSs which manages all POS from the merchant, StewardBankISave which manages all transaction that are done through ISave accounts, StewardBankBranchpos which manages all Point of Sales in all branches of Steward Bank, PEX which manages all VISA cards transactions for Steward bank and StewardBankMobileSnk which manages all mobile transaction be it wallet to bank or bank to wallet. When the Postbridge is down, all services mentioned above will be down and no transaction will be available to all this services.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**09-13 September**

**DESCRIPTION OF WORK DONE**

* Channels monitoring
* Banking jargon

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* In channels monitoring we have HSM loader balancer which is responsible for accepting pins. When the password is wrong it will decline the transaction and return a response code of wrong pin.
* The issuer is the one who provide the payment cards to the customers of the bank on behalf of the card networks that is, ZimSwitch and MasterCard. ZimSwitch provides cards which are used locally that is the payments cards are only used within the borders of the nation. In Steward bank, for a person to access such a card through you use the \*236# and create an account and issued the card after having deposited an amount of 10 rtgs. MasterCard are card issued by the bank to its customers which are mainly used to transact beyond the borders of the country. For someone to access the card he/she has to apply and after granted, will have to deposit 10 usd for the account to function.
* An acquirer facilitates payment card transactions on behalf of merchants. The merchant is a company registered through a bank for example pic and pay merchant. The acquirer is the one who owns the account of the merchant where the money goes after a customer does a transaction through a point of sale (POS). Where there is use of the point of sale it is known as the acquirer.
* **Payment Card Association** are cards which are mainly used in the payment of goods and services beyond the borders of the parent country. A bank card association is an organization owned by financial institutions that licenses bank credit card programs. The organization are which gives the license are known by the name Visa and MasterCard. For a company to use these association cards, it has to pay a certain fee to access the privileges associated with the card associates. After paying the company will be able to access and use the company name and the cards which are owned by the organization. The card associations gives the card owner privileges to transact to any company within and beyond the borders of the country.
* **Payment Switch** are switches which are used to communicate with from the point of sale to the banking account. It facilitates the validation of the payment card that is validating if the password entered is correct and also checking the name or the details of the card holder. Postilion and Sparrow are one of the example of payment switch. In Steward bank we use postilion which uses post card to show the details of the card that is, the name of card holder, the card number and the account number which is used to link with the account in the banking system where the deduction of the money in the account will take place. It also uses the HSM loader balancer is used to validate that is, checking if the password enter is correct so that the transaction process will continue.
* **ZimSwitch** is an organization that integrates all the banking institutions that is if a steward bank card is transacting on the POS of Stanbic bank, the ZimSwitch is responsible for linking the card with the Steward bank account using the Bank Identification Number (BINs) that is 502195 for Steward bank accounts. It is responsible for issuing cards for use locally that is the cards will be carry money which transact locally. BINs contains the first six digits that appears on the primary account number which will show where the transaction belong for example CBZ BANK LIMITED starts with 601237 and FBC BUILDING SOCIETY starts with 504992.

**A sequence diagram for a POS ZimSwitch transaction, that is how a transaction that is done by a CABS customer done on our Steward Bank POS gets routed (get Visio installed on your machine)**



* From the customers point, the customer swipes his/her CABS card on a POS owned by Steward Bank. The POS will send a request to the postilion and the postilion will check if the card belongs to the Steward bank or not. In this case it does not belong to the Steward bank and the postilion then sends request to the ZimSwitch. The ZimSwitch will be able to direct the request to the CABS account through the use of the Bank Identification Numbers (BINs). The CABS contains 588892 on its first digits of Pan Number which the ZimSwitch will use to connect to the CABS bank. It then sends request to the CABS bank were the cabs will check the validity of the card, the sufficient balance for the transaction and also it will check if the pin entered is correct. If it is valid then it will the CABS will deduct the amount transacted and then it sends response that the account has been deducted and the transaction was successful.



* If the bank does not send the response to the bank at a given time it will reverse the transaction that is it will send the reversal request to the bank as shown in the diagram above. The bank will reverse the transaction that it did in the cardholder account and then issues the response from the bank to POS machine where the customer has made the payment.



* The message is sent from the point of sale then goes through postilion and the postilion will check if the card is a Steward bank card. If it is not a steward bank card as shown in the diagram it then sends the message to ZimSwitch but when the service is down, it then sends a response to the point of sale showing mostly a response code of 91 which is Switch inoperative.
* **Prepaid Cards** are cards that are loaded with hard currency that is mainly the usd currency. These cards gives you access to purchase goods and services beyond the borders of the mother country using plastic money. As Steward bank we mainly use the visa branded card and MasterCard. These cards will be under the Steward bank and every transaction that happens is controlled by PEX which monitors the flow of each and every transaction which is done using these prepaid card.
* **Debit Cards** are cards which are used by customers to transact using the local currency. Most of these cards are owned by an organization called ZimSwitch. In simple terms this is the plastic money used to transact in the local markets and cannot be used to transact markets that are beyond the border of the mother country. These cards are the same as the prepaid cards but the difference is that they are used to carry money in local currency. The money is immediately transferred directly from the cardholder's bank account when performing any transaction.
* **Credit Cards** are cards which allows a customer to purchase his/her goods on credit and the amount credited has to be redeemed in the agreed time with the bank. The card issuer creates an account which enables the customers to by the goods and services on credit and grants a line of credit to the customer of the bank, from which the customer can borrow money for payment to a merchant.
* **EMV card** stands for Europay MasterCard and Visa cards. It is a chip embedded card which was designed to enable secure payment at compatible point of sale (POS) terminals. When the card holder inserts his card for payment, the terminal communicates with the card issuer's system for authentication and a single-use transaction code is issued that is the card will be used to transact at most for a single time. EMV cards can also support contactless payment through near-field communication (NFC) wireless connectivity. Near Field Communication (NFC) is a wireless connectivity standard that uses magnetic field to enable communication between devices when they're touched together. When the chip gets in contact with the point of sale, it then creates a unique code for each transaction and sends that code through the credit card processing system to authorize the transaction. This will make it difficult for the card cloner to access the information about the card since there is a different code sent on every transaction. After the code has been used it cannot be used again.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**16-20 September**

**DESCRIPTION OF WORK DONE**

* Report creation for daily transactions.
* Channels monitoring

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* We will be creating daily reports which contain the following information type of transaction, amount in the transaction and number of transactions on the transaction type for example on banking services, Balance inquiry, Mini-statement inquiry, Wallet to Bank and Withdrawal
* On channels monitoring we experienced disconnection on some of our server like postbridge and transaction manager. We restarted these services through connecting to the server remotely using remote connection which is used to login to the server. In the server we use windows 2012. For us to restart the services we use the start menu in the operating system, then search for services so as to restart the services. There are some cases which will require us to restart the whole server when the services are disconnecting several times. The cause of these disconnection where due to much space being taken for the services to function

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

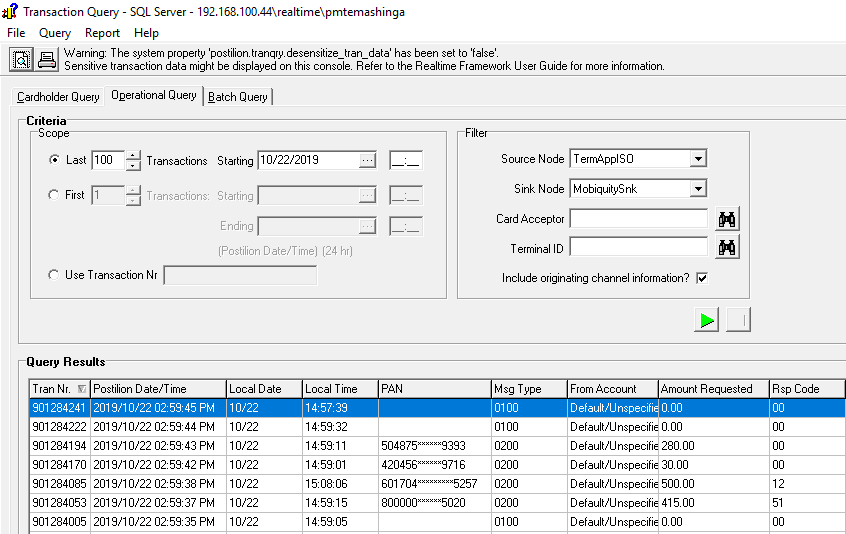
**23-27 September**

**DESCRIPTION OF WORK DONE**

* Recording of channel queues.
* Transaction Checks

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* In the channels queue, we recorded after every 15 minutes so as to know if our systems are running properly. For channels with a zero queue are available, our services will be running properly but when the queue value is more than zero, the services will not be functioning properly. The services that we will be recording are STEWARDVISA, STEWARDMastercard, SBZISave, Banking Services, ATM, BranchPOS, MOBILE, POS Notify and POS.
* We used the Realtime Management console to reveal all transactions on different source nodes that is, were the transaction starts and sink node were the transaction should proceed to for example, SBZMobileSrc source node which is responsible for all mobile transaction and SBZMobileSnk sink node is the link between the number and the account and it is responsible for mobile transactions, balance inquiry, internal transfer and requesting for Mini-statement, TermAppISO source node is a node for all steward bank point of sale and SbzIsaveSnk node is responsible for all ISave account and it is responsible for transaction on goods and services, Change of PIN and balance inquiry, TermAppISO source node with MobiquitySnk node which is responsible for all phone transactions and it is responsible for Non-cash transaction for example, wire transfer from swipe to ecocash and balance inquiry on the merchant and TermAppISO source node with ECOSALEREST is responsible for all transactions in which the customer inserts his/her Ecocash number on the point of sale sending a message to the mobile requesting for a pin for the transaction to become a success. When the response code is showing 00 on the transaction, this will show that there are no challenges on the transaction. When the response code is 91, some of the services that makes the transactions to flow will be down making it difficult for the transaction to be a success. There are many response codes that are seen on most of the transactions such as 05 which is ‘Do Not Honor’, 51 not insufficient funds, 68 response received too late and many others. We check these transactions through the Realtime Management console as shown below



**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**23-27 September**

**DESCRIPTION OF WORK DONE**

* Windows installation
* Channels Monitoring

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* We took a bootable flash disk for us to install the windows. We followed the whole steps from choosing the type of windows, formatting the whole computer for us to install operating system. We waited for it to complete the whole process of coping files and installation. We set the username as admin for all computers with a similar password. We then gave it a domain name for Steward bank when we had logged in on the steward bank WIFI then restart the computer for it to be registered on the domain. After all these processes we were now good to go. We then install office 2013, adobe reader, anti-virus, chrome and skype.
* On channels monitoring we experienced disconnection on some of our server like postbridge and transaction manager. We restarted these services through connecting to the server remotely using remote connection which is used to login to the server. For us to restart the services we use the start menu in the operating system, then search for services so as to restart the services. There are some cases which will require us to restart the whole server when the services are disconnecting several times.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**30 September-4 October**

**DESCRIPTION OF WORK DONE**

* Disconnections on services

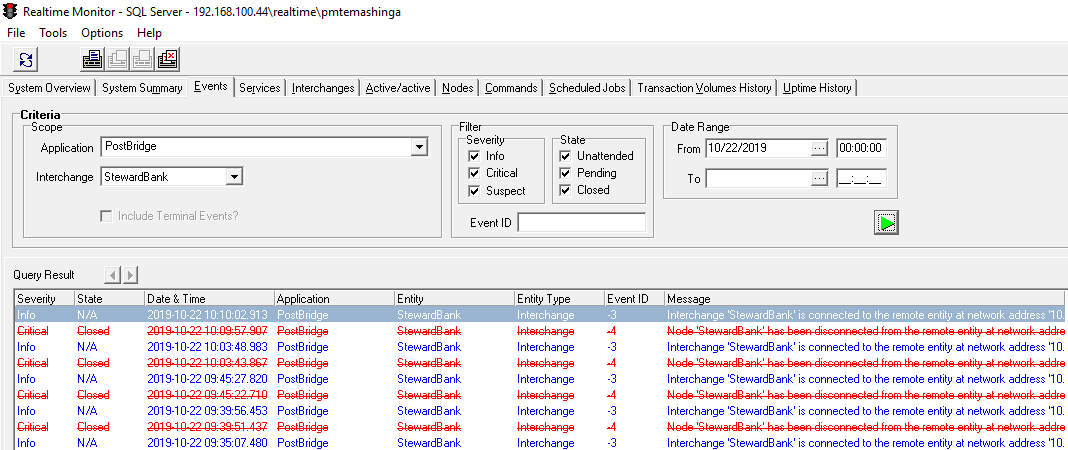
**SKILLS APPLIED/ NEW SKILLS LEARNT**

On disconnections I leant that, for a system to disconnect, it has to timeout for a number of times in a role. In Isave, when five timeouts have been experienced by the console, this makes the Isave services disconnect. When the Isave disconnects for only five minutes, any Isave card holder will not be able to make any transaction in those five minutes. ZimSwitch times out for five times in a row, the ZimSwitch services will disconnect and restarts itself and the time space between the disconnection and auto-restart of the service will be less than a second but any non-Steward bank cardholder that transact through a Steward bank point of sale will not be able to transact on that disconnection space of time. In T24 accounts that is StewardBank interchange, when five timeouts have been experienced by the console, this makes the StewardBank interchange services to disconnect and then restart itself automatically after disconnection. When the StewardBank disconnects for only five minutes, any T24 card holder will not be able to make any transaction in that disconnection timeframe.

We can also check the disconnection of all Steward bank point of sale from the PostBridge application. All services connected to the PostBridge application disconnects after experiencing five timeouts in a row. Such services are as follows StewardBankBranchPOS which manages all transactions that are transacted on a steward bank point of sale, StewardBankATMs which manages all ATM owned be the steward bank, StewardbankMobileSnk which manages all steward bank transactions through mobile be it transfers through the Ecocash and through \*210#, STEWARDBANKAGENTPOS which is responsible for all agents point of sale, STEWARDHomesend which updates merchants account with ZimSwitch and StewardBankPOS manages all transactions that flows through all point of sale owned by the bank. StewardBankPOS manages transactions that are from Steward bank’s customer or that are from other financial service provide that goes through the ZimSwitch gate, which will check the bank identification number showing the bank of the card transacting.

We were also checking the transaction manager disconnection which is the root of all transactions and services managed by postilion. When transaction manager disconnects, all services will automatically disconnect and any company that will be using these services will face some challenges when transacting. It may disconnect main because of space that it will be using for it to function. The space might become very low due to many transactions flowing through the transaction manager. For us to restart the server, we had to log in the server were the postilion was installed then restart the service through the server. It would disconnect itself after restarting it and this was due to queues in the TermAppISO that arise through the disconnection period. In this issue we had to disconnect the TermAppISO through the server so as to freely start the Transaction manager without any challenges, then after some minutes we would restart the TermAppISO.

To access these disconnections, we used the real time management console and access this disconnections through the events section as shown below:



All the information that is cancelled as shown above shows the time when the service was disconnected and the information that is not cancelled shows the time it restarted itself.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**07-11 October**

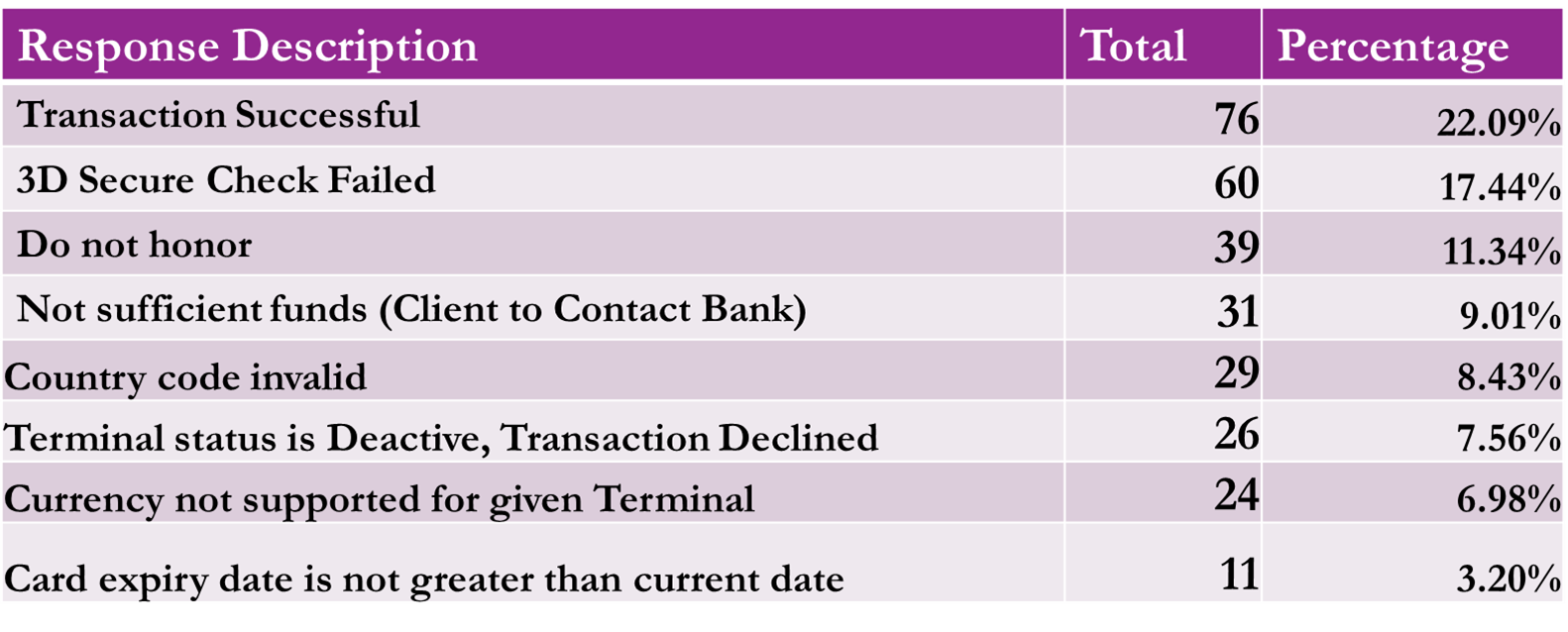
**DESCRIPTION OF WORK DONE**

* **Research on failed Transactions on the E-Commerce**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

**Acquired E-commerce transactions**

Acquired transactions in this case are Steward Bank merchants being used in the transaction of goods and services. Merchant is any organization that receives payments for goods or services. On the acquired e-commerce transaction, the following is the summary of the transaction for a period of six months;

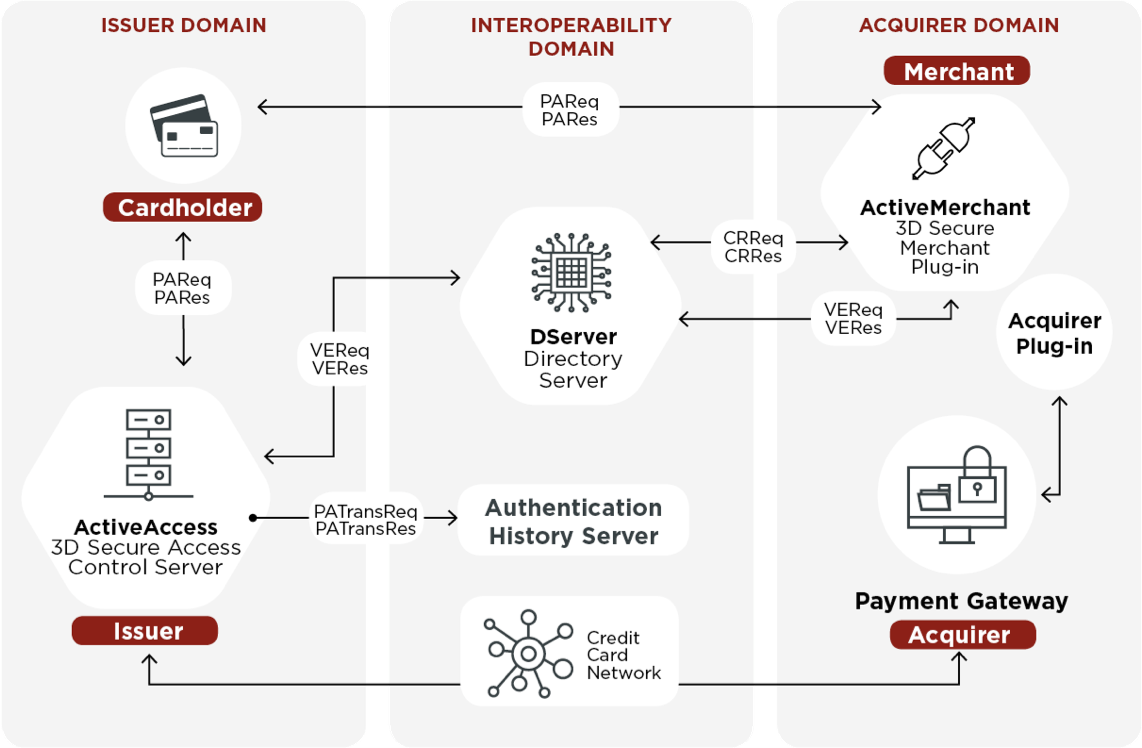


3D secure check failed

On 3D secure check process, when the card holder transact on a terminal with 3D secure, it send a message to the card scheme's Directory Server, which holds a directory of all the BIN ranges corresponding issuing banks. The Directory Server will receive the message from the Merchant Plug-In (**MPI**), check the card number against the BIN range directory that it holds for example Steward Bank VISA cards starts with **463833**, and forward that message onto the correct issuing bank. The issuing bank would then proceed with authenticating the card user. In the issuing bank, it uses the Access Control Server (**ACS**) which contain the details of the cards that are registered on the 3D secure for authentication. ACS will check for card details of customers that are listed on the 3D secure. When the card details are not registered on the ACS it then decline the transaction and gives a response code of 3D secure check failed. If the card is registered on the 3D, an OTP is then send to the cardholder’s email address for the transaction to be processed. The transaction will then go to acquiring bank to debit the cardholder account and credit the merchant account.

As a solution to this problem, we held a meeting with the e-commerce managers. All cards were not yet registered on the Access Control server and it was a work in progress. After the meeting we had to communicate with the cardholders of Steward Bank Visa cards to confirm if the details for the card are correct such as the email and phone number, so that the company will be able to send the On-Time password that is the OTP for the transaction to be a success.

This is shown in the diagram below:



There are some instants in which, someone can transact through a merchant which has no 3D secure plugged in, the transaction will flow through the merchant and goes through the acquiring bank to credit acquiring bank and debiting the card owner account.

Do not honor

A do not honor notification means that the customer's card issuing bank has temporary hold the card. This may be because of multiple decline on a transaction that is multiple wrong pin will force the issuing bank to hold the card. It may also be caused by failing to put the exact CVV2 number which is the Card Verification Value which is used on all online transaction. It is a three digit number which is the last three numbers in the signature space on the back of the card.

As a solution, customers are to be educated on how to purchase goods online that is the expiration date of the card, were to get the CVV2 number and the card number. Trials required on inputting the On-Time password so as to prevent card hold on the card which will give a do not honor response when transacting.

On ‘**Not insufficient funds**’, the customer will be transacting without having the knowledge of the charges that correspond with the transaction which customer wants to take. These charges will be on all transactions that are done online and they will add an extra amount on the price tagged on the goods and services to be purchased. On ‘**Invalid Country Code**’, the terminal might be registering a 932 for Zimbabwe country code whilst the country code on the bank card will be ZWL or the other way round.

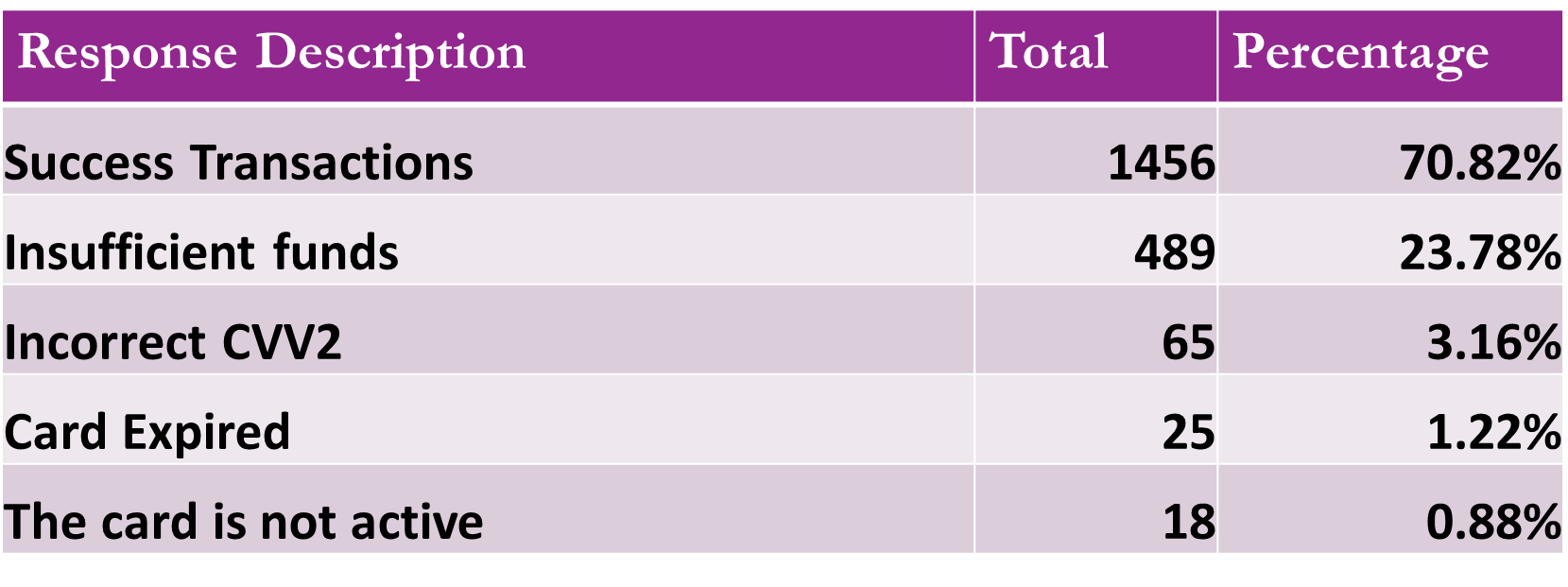
Terminal status is deactivated

A terminal is an online page used to make payment. It will require card number, expiration date, CVV2 number and the billing ZIP code. According to the research, the terminal that was deactivated is BUXTON CARTER which is a terminal that was deactivated because of high cases of fraud. Fraud involves hiding of information or providing incorrect information for the purpose of tricking victims out of money. These terminals where deactivated because many people were losing their many through the page.

Currency not supported on given terminal simple means that the current terminal will not be accepting the currency being used by the VISA card for example, the terminal will be accepting euro whilst the VISA will be transacting using USD as its currency. Lastly, the client will be purchasing with an expired card that’s why it will give a response code of ‘card expiry date is not greater than current date’.

**Issued E-commerce transactions**

Issued transactions in this case are Steward Bank customers transacting on merchants owned by other companies such as DSTV and Amazon. On the acquired e-commerce transaction, the following is the summary of the transaction for a period of six months;



**Not insufficient funds**

The customer will be transacting without having the knowledge of the charges that correspond with the transaction which customer wants to take. These charges will be on all transactions that are done online and they will add an extra amount on the price tagged on the goods and services to be purchased.

**Incorrect CVV2**

This CVV2 number is a requirement code for every online transactions and it is the three-digit number printed in the signature space on the back of most credit cards, such as Visa, MasterCard, and Discover cards. The CVV2 number is always the last group of numbers in the signature space on the back of the card. It is not part of your regular credit card number. Customer might not have the knowledge of where to find the CVV2 number and as I have research many people acquire for these cards with the intention to transact online without full knowledge of what is required for one transact online. As a solution, customers are to be educated through sending an email which will be thanking the customer for opening an account with the bank, the bank then add a message which gives the information on what is required to make an online transaction that is, the card number, the expiration date and the CVV2 number with a picture showing where to get the CVV2 number.

On ‘**Card Expired**’, some terminals will record the expiration of the Visa card when it is the month of expiration for example if the expiring date of the card is 12/19, when the current date is 01/12/19, the terminal will be recording that the card has expired. On ‘Card not yet active’, these were the cards that were issued before the system was introduced. Their details were not captured into the system so the cards were being recorded as not being active.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**14-18 October**

**DESCRIPTION OF WORK DONE**

* **Resetting password on the Steward bank portal**
* **One time password**
* **Access directory Server**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* In the steward bank portal, many users would easily forget their password and to clarify if they are Steward Bank employees or not. In the process of putting wrong password and putting a correct password and not clarifying that it is a Steward employee, led to their accounts being locked. Employees with locked accounts had to send an email requesting for a password reset. When resetting there password I used a unique password for all who had requested a password reset which was easy and short like “password” for easy to remember because some would call and I had to reset over the phone due to how quick the user wanted the password. After resetting the password, some would face challenges on setting a new password because after resetting the password, the portal will request a new password. Some will face challenges on setting the new password, so I had to remind them on what is required in a password such as uppercase, lowercase, characters and no repetition of previous passwords. Some would face challenge on putting the password following the password required password. I had to re-reset their password so that the employee will be able to put a new password as requested by the portal.
* . One-time pin or dynamic password, is a password that is valid for only one login session or transaction and some are sent via mobile as a way of verifying if you are the owner of the card with the contact details you registered your card with. When a customer purchases a good or a service, for the process to complete a message is sent to the customer which contains an OTP which will complete the transaction. This one-time password will then complete the whole transaction process. Once this one-time password is used, it will no longer be re-used again or given to the same person as a one-time password.
* An access control system (ACS) is a type of security that manages and controls who or what is allowed entrance to a system, environment or facility. It identifies entities that have access to a controlled device or facility based on the validity of their credentials. In Steward bank we use this service for capturing all our customer details for 3D secure verification. When a Steward bank card holder transact, the transaction will move from the point of sale to directory server which contains range of all card numbers that are registered in the 3D secure and after that the transaction then goes to the access control server where it will check for the email to send the one-time password.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

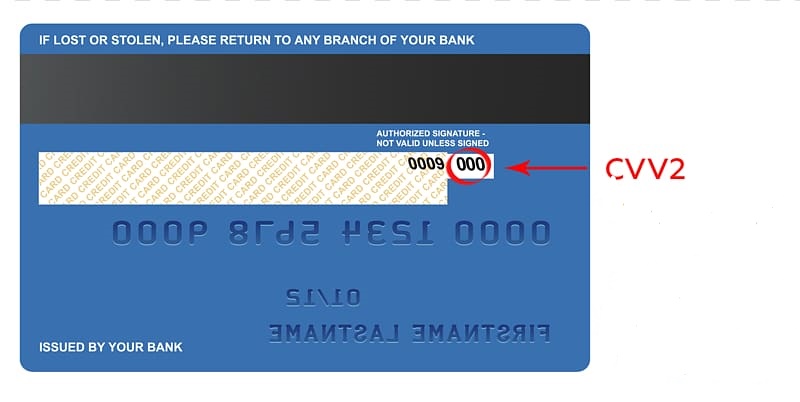
**21-25 October**

**DESCRIPTION OF WORK DONE**

* **Card security codes**
* **Agile process**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* The Card Security Code is usually a 3- or 4-digit number, which is not part of the credit card number. These security codes are used or all online transactions as a way to establishing the owner's identity and minimizing the risk of fraud. It is required to complete transactions using cards, but along with that, it also provides added security against scams. VISA cards have their security code on the back of the card on the signature box. It is the last three digit of the number that is the last three digit that appear on the number that is on the back of the card. MasterCard security code is also a three digit number that is found on the signature box on the back of the card. It is also known as the CVV2 (Card Verification Value) and it is used to prevent e-commerce fraud. The customer proves that he/she is in physical possession of the card at the time the transaction is taking place. For Visa and the MasterCard, the security code is found on the back of the card as illustrated in the picture below:



These are also the last three digits of the numbers behind the card. Amex (American Express) security code is the four digits that are found on the front of the card just above and on the right of the cards. It is also known as the CID (Card Identification Number) and it is used to prevent e-commerce fraud. The customer proves that he/she is in physical possession of the card at the time the transaction is taking place. For AMEX the security code is found on the front of the card as shown in the picture below:



* I leant that a project owner gives his or her requirement on a particular product and gives it to the project analyst. Project analyst will be responsible for creating the process in which the product will follow that is from point of sale up until the point of debiting the customer account if this product is a payment platform. The project analyst is also responsible for making conclusion if the project is feasible and if it will bring revenue to the business as a whole. Project analyst will then forward the project to the Scrum Master who will look if the project can be done using the available resource and also if the project is realistic and achievable. The scrum master then sets the time in which the product is expected to be in the market. When all the process is done the development team will then develop the product and when they are done it is then given to the users for use. These users will then determine if there is need of an update depending on how satisfied they are with the product. If there is need of an updated as per user request, they will redo the process of creation of the new product up until the user of the system is satisfied. In the Agile process, products are produced faster into the market and these products will be upgraded gradually as they progress.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

**28 October – 1 November**

**DESCRIPTION OF WORK DONE**

* **EMV**
* **Magnetic Stripe Card**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* EMV is an abbreviation which means Europay, MasterCard, and Visa. These are the world dominate the sector and developed the global standard for chip-based security. An EMV card has an embedded microprocessor or a chip that is used to interact with merchant to make sure that the card is valid. These EMV cards are cards which have an embedded chip which is used as a security measure when transacting on a point of sale. These chip cards are secure in the case that when the card holder insert the card on a point of sale, the point of sale will generate a unique code which will be used by the point of sale. This code is used to decrypt the card holder details on the chip and this code is only used once to decrypt the information that is if the hacker captures the code as given by the merchant he is not able to reuse it again. EMV were put in place to reduce card cloning. Card cloning is a process of making another copy of the same card. The cloned code will be carrying all the information necessary for someone to make a transaction that is, the card number, the name of the card holder, the expiration date of the card and the service code. These information will be used by the card cloner to gain access of the card and start transacting using the card using the pin of the card as produced by the merchant.



A magnetic stripe card is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. A magstripe reader understands and is able to read every information on the magnetic stripe of the card. On a magstripe there are three tracks that contain the card holder information.

**Track 1**

Track 1 contains the start sentinel which is a character used to indicate beginning of a block of information. It also contain the PAN number (Primary Account Number) which is up to 19 characters and is usually, but not always, matches the credit card number printed on the front of the card, the first name and the last name of the card holder, the country code that is +263, a separator, four digit expiration date of the card, service code which contains three digits and discretional data which contains the CVV number. On service code the three digits contains the following:

**First digit between (1, 2, 5, 6, 7, 9)**

1: International interchange OK

2: International interchange, use chip where feasible

5: National interchange only except under bilateral agreement

6: National interchange only except under bilateral agreement, use chip where feasible

7: No interchange except under bilateral agreement (closed loop)

9: Test

**Second digit between (0, 2, 4)**

0: Normal

2: Contact issuer via online means

4: Contact issuer via online means except under bilateral agreement

**Third digit between (1 - 7)**

0: No restrictions, PIN required

1: No restrictions

2: Goods and services only (no cash)

3: ATM only, PIN required

4: Cash only

5: Goods and services only (no cash), PIN required

6: No restrictions, use PIN where feasible

7: Goods and services only (no cash), use PIN where feasible

For example

%**85338407000278761**^**MONEY SAFE**^*1306*226100000001000000**882**000000?

For the card below this is the description of the data taken from track 1:

* 85338407000278761 is the card number.
* MONEY SAFE is the cardholder name.
* 1306 is the expiration date.
* 226 is the service code.
* 882 is the discretion number.

**Track 2**

Track 2 contains the start sentinel which is a character used to indicate beginning of a block of information. It also contain the PAN number (Primary Account Number) which is up to 19 characters and is usually, but not always, matches the credit card number printed on the front of the card, the first name and the last name of the card holder, the country code that is +263, a separator, four digit expiration date of the card, service code which contains three digits and discretional data which contains the CVV number. On service code the three digits as explained in the track 1 part. On top of these features same features as contained by track 1 it also have longitudinal redundancy check (LRC) which is one character and a validity character calculated from other data on the track. Most reader devices do not return this value when the card is swiped to the presentation layer, and use it only to verify the input internally to the reader.

**Track 3**

The following data is stored on track 3:

* Template V#
* Security V#
* Postal Code
* Class
* Restrictions
* Endorsements
* Sex
* Height
* Weight
* Hair Color
* Eye Color
* ID#
* Reserved Space
* Error Correction
* Security

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

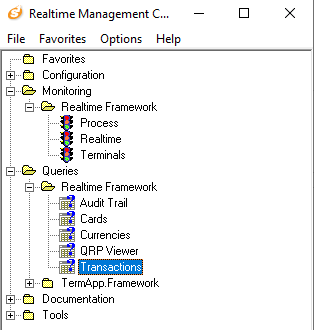
03-08 November 2019

**DESCRIPTION OF WORK DONE**

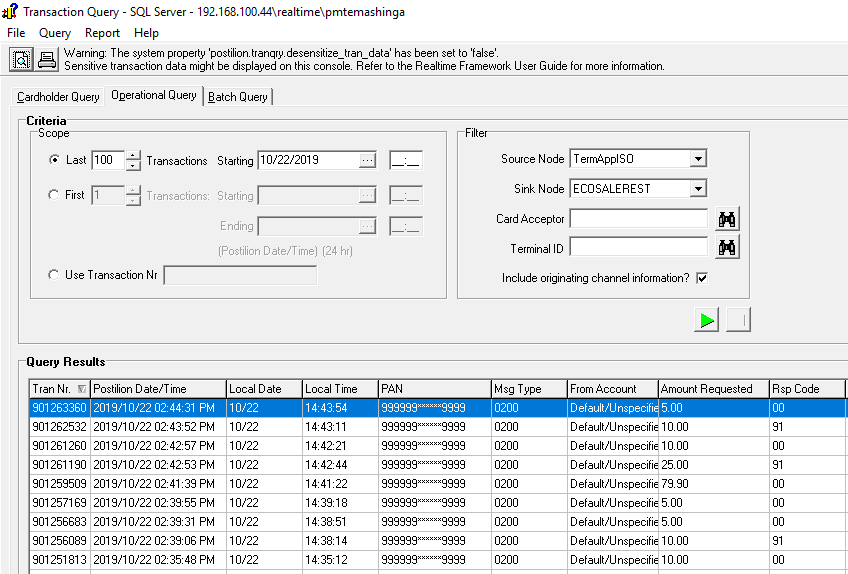
* **Creation of a beginner’s manual**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* I created a manual which contained every daily task that an employee is expected to do on a daily bases. The manual showed how to ping a server using the command prompt where we will type ping 1000.10000.45.1 –t to have a continuous flow of these servers. By pinging a server, we will be checking if the server available and is active. We mostly pinged four servers which we were mainly using on a daily basis. If a server was down we usually see it with multiple timeouts from the ping and this could affect our flow of transactions. When a server is down a person who will transacting might face some challenges having an error of do not honor or Issuer Or Switch Inoperative meaning the issuer might be off for reasons beyond their control. Server may disconnect due to network issues that run these servers which will make these server inaccessible. There was also transaction checks on the manual. This was to guide an individual on how to access all the transaction using the source node and the sink node. We used real time to access these transactions as shown below:



To access the transaction query, we select the queries option then select realtime framework to have access to transactions. In transaction, we will have access to all transaction checks. When the transactions have 00 as their response code (rsp code) where 00 means approved or completed successfully, this will show that transactions are flowing and nothing is wrong with the services as shown below:



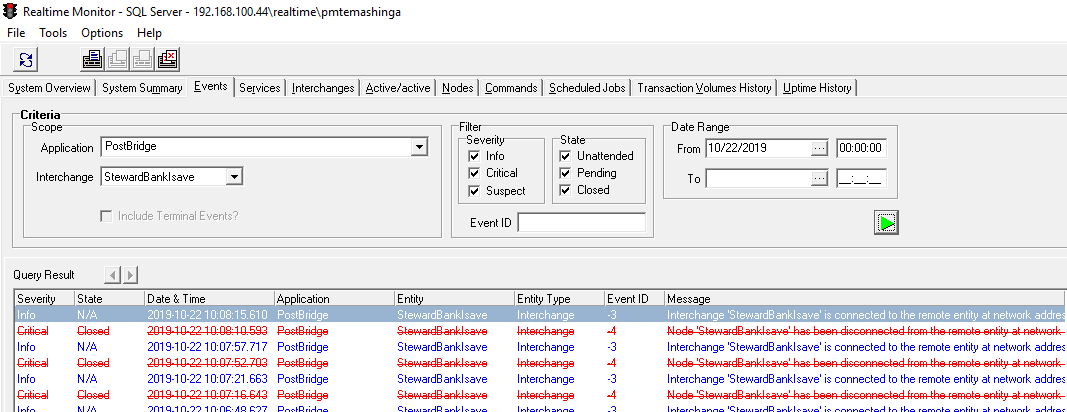
As show above more transaction are completing with a response code of 00 which means transaction approved. This will show that the system is performing well and there are no challenges with the system. The following are types of transaction check on the beginner’s manual:

In the above transaction check, the source node is Termapp which is responsible for all point of sale and the sink node is ECOSALEREST. This is a transaction check for all Ecocash point of sale transactions where by the customer puts his or her Ecocash number on the POS then a message will pop up on the mobile requesting for Ecocash pin.

Still on source node of TermAppISO there was also a sink node of SbzIsaveSnk and this transaction check is for all Isave account that transact through any of our point of sale at any selling point.

There was also a sink node of SbzPexSnk on TermAppISO and this transaction check is for all Visa card transactions on all Steward Bank point of sale be it Steward bank card or any other VISA card owned by other financial institutions. On the source node TermAppISO there is sink node of StewardPOS which checks all transaction of Steward bank cards whose cards are in T24 that transact through Steward bank point of sale. There are many transaction checks in the beginners’ manual but I have just mention a few.

There was also disconnection checks on the services managed by the postilion in which all transaction are managed. The following is an example of such disconnections:



All cancelled results shows the disconnection on a service. On the above diagram, I was checking the disconnection on the StewardBankIsave linked to an application called Postbrige which manages most of our services owned by Steward bank. It shows that the service has disconnected from the service for a minute caused by multiple time outs on the remote server.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

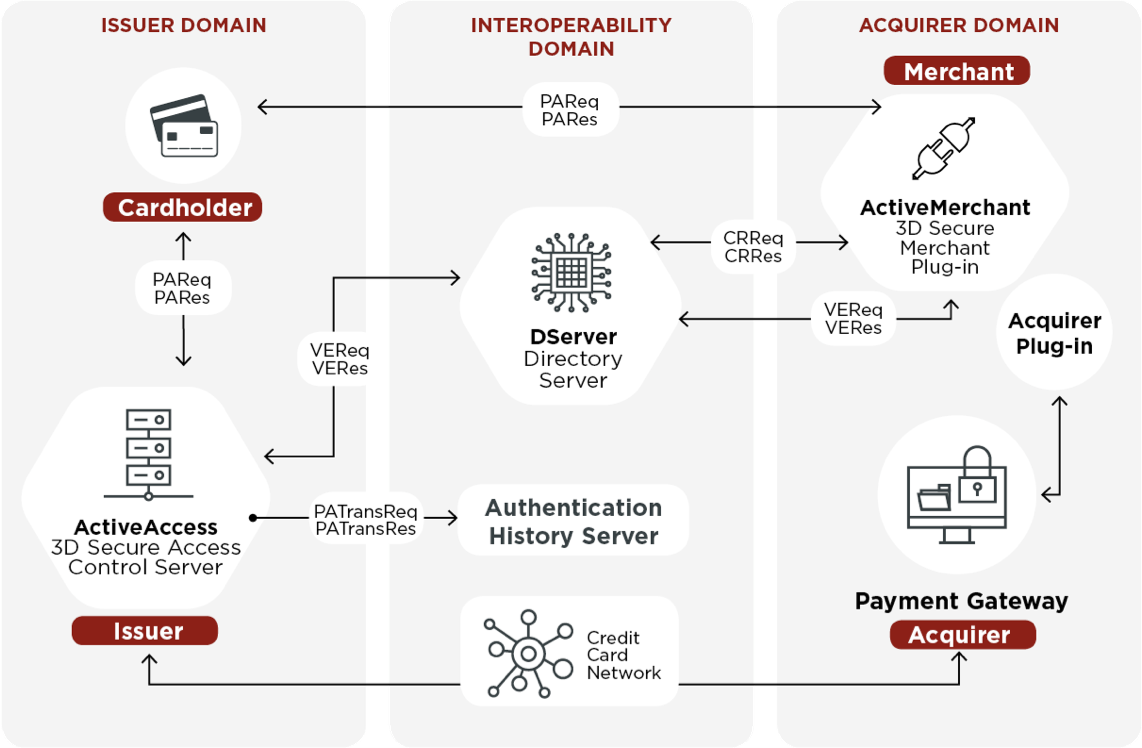
11-15 November 2019

**DESCRIPTION OF WORK DONE**

* **3D secure**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* 3D secure is a security protocol which help to prevent fraud on online transactions where fraud is any act of deception carried out for the purpose of unfair and unlawful gain. In fraud, a person can use someone’s card to transact if there are no passwords required on the terminal. 3D secure was introduce to make all transactions that are done online to be more secure through the use of a one-time password (OTP). An OTP is the one sent via an email or through mobile to initiate the transaction. This password will be used once and it cannot be reused once done. The OTP is sent to the email in which the card holder registered with or their mobile they registered with. If a person tries to transact online with a card that doesn’t belong to them, the transaction will not go through since the one time password will have been sent to the card holder email. 3D means three domains and there is the Issuer domain, the Interoperability domain and Acquirer domain. The following diagram shows the 3D secure process involving all the domains:



* Issuer domain is the bank that issues its cards to the customers. It is responsible for capturing the details of the customer into the system and also registering the cards into the 3D secure system and in this case the customer details are uploaded in the Access Control Server. The Access control Server will contain all the customer details and it is responsible for sending an email to the customer after confirming and checking if the card is registered for 3D. In this email, that’s where the one-time password is contained such that the transaction may complete.
* Interoperability domain acts as ZimSwitch. It is responsible for checking the bank identification numbers of the card that need to transact online. It locates the card issuer institution using the bank identification number. If

a card transact online with the card number 4630330000000000, the directory server will check the first six numbers of the bank card and directs the transaction to the financial institution which own the bank identification number which is Steward Bank in the example.

* Acquirer domain is the owner of the merchant in which the transaction is initiated. It is responsible for sending a request to the directory server. Merchants that are 3D enable are safe for making an online transaction. If the issuer approves that the card is 3D secure, the merchant will then have access to debit the customer account and credit the account with the merchant. If the card is not 3D secure registered, it then sends an error message of 3D Secure Check Failed.

**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

18-22 November 2019

**DESCRIPTION OF WORK DONE**

* **VISA card deposit**

**SKILLS APPLIED/ NEW SKILLS LEARNT**

* When depositing money into a VISA card, the bank teller first checks if the card is not expired and if it is expired, the teller will advise the depositor to purchase a replacement card so as to deposit the amount of money the depositor wants to deposit. If the card is still valid, the bank teller will check if the account is active in the PEX system which manages all VISA account. If the account is active in the PEX it is then funded into the PEX account of the card holder and then credit also the T24 account. After that, the deposit slip is then forwarded to the back office where it will be approved by the supervisor. The supervisor will check if the amount credited to the account is the same and also if it was the correct account in which the money was deposited. When the deposit has been approved it will then reflect into the account. If the account is not active, they then deposit to PEX suspense account clarifying the account in which the money is to be deposited so as to update the account that is, the missing details and activation of the card. When the account is active, for the money to reflect into the account it might take 15 minutes at most to reflect into the account and if not active, the money will reflect in 30 minutes at most.



**SUPERVISOR COMMENTS**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**STUDENT’S SIGNATURE** …………………………… **Date**…………………

**SUPERVISOR’S SIGNATURE**………………………… **Date** ………………..

25-29 November 2019

**DESCRIPTION OF WORK DONE**