2018

A Collaborative tool to prevent fraudulent usage of financial cards

Wilson N. Gitau
Faculty of Information Technology (FIT)
Strathmore University

A Collaborative Tool to Prevent Fraudulent Usage of Financial Cards

Gitau, Wilson Ndungi

Dissertation submitted in partial fulfilment of the requirements for the Degree of Master of Science in Information System Security, Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

May, 2018

Declaration and Approval

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Name of Candidate: Mr. Gitau, Wilson Ndungi

Signature:

Date: 28th May 2018

Approval

The dissertation of Mr. Gitau, Wilson Ndungi was reviewed and approved by the following:

Dr. Vitalis Gavole O,
Senior Lecturer, Faculty of Information Technology,
Strathmore University

Dr. Joseph Orero,
Dean, Faculty of Information Technology,
Strathmore University

Professor Ruth Kiraka,
Dean, School of Graduate Studies,
Strathmore University

Abstract

Technology usage has advanced a great deal in banking and telecommunication sectors. With the continuous improving infrastructures in information technology, new technological dimensions have been opened up to ease processes in these sectors, for example people do not travel to pass communication, to shop and in banking people do not necessarily walk in to the banks to facilitate their financial transactions. Despite this advancement there are dire consequences of possible fraud or crime when we lose our banking identity documents and financial cards. Compromised, lost and stolen credit cards, debit cards, SIM cards, identity cards can be used in crimes. Due to vast adoption of this technology it has increased the surface of this kinds of crime, thereby causing financial loses and posing a challenge when tracking and preventing fraudulent events of the compromised financial cards.

This study proposes and implements a system that: prevents fraudulent usage of compromised and lost financial identity items. These items include credit cards, debit cards, and SIM cards. The system will work towards assisting the authorities in investigating crime caused by financial cards. The system provides a blacklist API to the card industry, banking, merchant's systems and individuals to backlist lost financial identity cards, an alert interfaces that reports usage of blacklist financial cards and a comprehensive reporting tool that helps in investigation of the crime. Agile methodology was adopted as the software methodology for the solution development. A prototype was developed to test the proposed solution. The system was populated with the relevant sample data for evaluation and validation.

Keywords: Fraud, API, Credit Card, Debit Card, Crime.

Acknowledgements

I would like to acknowledge those who enabled me to successfully complete this research project.

I thank God for the guidance, encouragement and grace He has shown me throughout this course, up until its completion with this dissertation.

I express my sincere and deep gratitude to my supervisor Dr. Vitalis Ozianyi for the invaluable guidance and support.

I extend sincere thanks to my colleagues and friends Patrick, Jacqueline, Felix, Chandi, Samuel and Prisca for their input, encouragement, their remarks and motivation.

Finally, thanks to my entire family: mum and dad for your support and always encouraging creativity in me, Travis, James, Eric and Josephine for always standing by my side.

Table of Contents

List of Figures

List of Tables

Abbreviations/ Acronyms

API	**-**	Application Interface
AVS	–	Address Verification System
B2C	–	Business to Customer
CVM	–	Card Verification Method
GUI	–	Graphical User Interface
HTML	–	Hypertext Markup Language
IDE	–	Integrated Development Environment
PCI	–	Payment Card Industry
PHP	–	Hypertext Pre-processor
PIN	**-**	Personal Identification Number
SDLC	–	Software Development Lifecycle
VbV	**-**	Verified by Visa
VPAS	**-**	Visa Payer Authentication

Chapter 1: Introduction

1.1 Background of Study

Over the past decade, there has been a great advancement in the utilisation and availability of information technology by the general population. This has rapidly improved banking processes and eased communication. These improvements have helped in the growth of online businesses (Aliyu & Tasmin, 2012). According to Smart Insights (2017), the latest ecommerce figures indicate that it's a booming industry, year on year online sales continue to grow expected to reach an astounding 1,115 billion dollars by the end of this year. An example of this advancement is in Kenya where ecommerce has been driven by a telecommunication mobile money platform called M-pesa. There is also a growing partnership in financial institutions and M-pesa provider where customers use various platforms such as M-Kesho, M-Shwari, M-pesa cards among others to transact and pay their utility bills (Nakhumwa, 2013). These mobile money technologies are now being adopted by the rest of the world to ease their processes (Ignacio & Radcliffe, 2011).

Despite the rapid uptake, identity fraud has become an ethical issue in this sectors (Joyner, 2011). According to Hedayati (2012), identity fraud is a crime where a person uses another person's personal information to benefit himself without their consent. The most common ways that lead to identity fraud are lost, stolen or compromised items such as banking cards and telephone calling cards. Compromisation of these items might be achieved by criminals engaging in shoulder surfing to get a glimpse of calling card numbers or credit card numbers, phishing and social engineering to get other people's card credentials. After obtaining these kind of information about a person, the criminal can take over the person's identity and is capable of conducting a wide range of fraud, for example fraudulent withdrawal from bank accounts, fraudulent purchase from online merchants and fraudulent use of telephone calling cards (Justice.gov, 2017).

Mandal (2014) Indicate that stolen and counterfeit financial cards contribute to more than 60% of fraud losses. As illustrated by Table 1.1 the highest percentage of credit card fraud is from lost and stolen cards.

Table 1.1: Methods of Credit Card Fraud and their Percentage of Occurrence (Mandal, 2014).

Method	**Percentage %**
Lost or stolen card	48
Identity theft	15
Skimming	14
Counterfeit card	12
Mail intercept fraud	6
Other	5

Telephone cards that is SIM cards have become a physical identity item on the mobile money platform. The introduction of mobile money helped poor people in developing countries access financial services offered by the traditional banking. The continuous embracement and adoption of mobile money platform by many countries across the world has increased the number consumers of financial services. People are able to transfer money, shop, payments bills among other financial services (Githui, 2011).

A stolen SIM card, whether physical or simply the access code gives the holder the privileges of the phone's owner and passwords access that could unlock more than just the physical phone. It can as well land in to crime scenes or even it might be used in co-ordinating communication that facilitates a crime (Meredith, 2017). Furthermore, the popularisation and the rapid adoption of the Internet has increased the surface of this kinds of fraud therefore crime investigation agents should keep abreast with this changing technology (Justice.gov, 2017).

With all the negative impacts of fraudulent lost identity items causing financial and product losses, fines and reputation loss to online merchants and service providers there is dire need come up with technological ways to combat this fraud (Shiv, Ayushi, & Mishra, 2015). This dissertation

proposes the development of system that provides a blacklist of compromised financial cards to the card industry stakeholders, thus preventing the fraudulent usage of compromised financial cards.

1.2 Problem Statement

With the changing consumer patterns and the adoption of Internet, e-commerce, e-banking, mobile money markets have rapidly expanded in the recent years, thus driving usage of identity items such as credit cards, debit cards and mobile phone cards (Nakhumwa, 2013). According to Visa Annual Report (2016), reports of 300,000 merchants with visa credit and debit card checkouts and is expected to double in the next two years. Safaricom reported growth of mobile money M-pesa platform having a customer base of 27 million + and over 130,000+ M-pesa agents (Safaricom Annual Report, 2017).

As this surface of financial identity items usage increase, so too have associated identity fraud levels: lost cards, stolen cards, compromised cards when in transit and counterfeit cards. As such identity fraud has become a significant problem, causing financial and product losses, fines and reputation loss to online merchants and service providers (Prabowo, 2010). Nilson Report (2016), shows that losses to card providers worldwide reached $15.72 billion, merchants $5.90 billion and card acquirers $6.12. It indicates that financial institutions are facing an ongoing battle to beat fraudsters while protecting their customers.

1.3 Research Objectives

i. To analyse aspects that drive digital identity theft in financial technology.
ii. To review the methods used to prevent and investigate fraudulent usage of financial cards
iii. To design, develop, implement and test a system that will prevent fraudulent usage of financial cards.
iv. To evaluate and validate if the system prevents fraudulent usage of financial cards.

1.4 Research Questions

i. What are the aspects driving digital identity theft in financial technology?
ii. What are methods used to prevent and investigate fraudulent usage of financial cards?
iii. How can a system that will prevent fraudulent usage of financial cards be designed, developed and implemented?
iv. Does the system prevent fraudulent usage of financial cards?

1.5 Scope and Limitation

This dissertation scope is to develop a prototype where incidents for compromised financial cards can be reported, it entails a collaborative building of a financial cards blacklist accessible via application interface to relevant stakeholders to prevent fraudulent usage. It goes to the extent of collecting feedback from stakeholders in case of attempted use or any detected signals of the compromised card and a reporting module that shows the traces of the compromised card. The research will mainly focus on the credit card and debit cards as the financial cards, other financial cards and financial identity items such as SIM card will easily integrate in future works.

1.6 Justification

Identity items are used to uniquely identify an individual. An individual will use his/her identity credentials to authenticate his/her transactions, it is a token of authorisation to access critical information thus if compromised, lost or stolen will cause harm to the individual account. A financial card is one of these identity items, it is used to authenticate financial transaction from your bank. If a financial card is fraudulently used might lead to financial losses extending to different parties: card owners, merchants, banks and card industry companies (Hedayati, 2012). In this case measures should be taken to prevent financial identity fraud and financial tokens such as credit cards, debit cards and telephone cards should be well tracked to prevent fraudulent usage.

Chapter 2: Literature Review

2.1 Introduction

Nowadays identity theft has rampantly increased. Financial cards being the most convenient ways of online payments pose a high risk of fraud when this cards are compromised or lost (Clough, 2015). In this chapter we will review nature and the usage of these financial identity cards, the crimes caused by compromised financial identity cards and latter investigate the methods that are currently employed to detect and prevent fraudulent usage of these cards.

2.2 Digital Identity Fraud

Digital identity fraud crimes have become more common, easier and safer to perform with little risk of getting caught. The introduction of the Internet access at home and business places, a new world was opened. The identity thieves in this era keep up to date with technology with their driving purpose been the enlarging e-commerce space (Shiv, Ayushi, & Mishra, 2015).

According to ftc.gov (2017) financial report, within 10 years of the advent of the Internet, 62% percent of the identity theft crimes were committed over the Internet. The crimes increased and became more sophisticated each year. It seems as the technology advanced, so did the thieves. Internet identity theft crime is very appealing to more criminals due to the physical and emotional distance. There is no risk of committing murder to claim a physical identity or being caught rummaging through bins to accomplish the crime goals. The lack of physical evidence made has it harder to catch the thieves (Hedayati, 2012).

Majority of the information comprise is done by use of malware, viruses and other methods to access computers illegally. It is quick and easy to transmit personal identifying information and sometimes, insecurely, through the Internet. Financial transactions are carried out online, access of credit card accounts can be done online, bills payments are done online, online shopping, money transfer and other services can all be achieved online in a convenient manner. The Internet enables the criminals to easily steal identities of different individuals from all over the world and use these information to access services legal to the victims such as loan applications, online purchases, credit card applications, cash withdrawal and transfer services (Prabowo, 2010).

2.3 Financial Cards

Financial cards are integral in the growth of the world's economy (Zareapoora & Shamsolmoal, 2015). There are different types of financial cards, namely debit cards, premium cards, store credit cards, charge cards, co-branded cards, unsecured credit cards, secured credit cards, affinity credit cards among many more. A debit card allows a consumer to pay for his goods and services against his bank account balance or savings whereas for a credit card the consumer is borrowing an amount to be paid later. All the above mentioned credit cards are designed according to the customers need and they also differ in their credit limit (GreenPath, 2018).

2.4 Financial Cards Network Structure

According to Akers (2005), financial cards transactions in goods or services payments go through a network of stakeholders: consumer, merchant and the financial institution (bank). This is as illustrated in Figure 2.1. The completion of goods or services payments from consumer to the merchant is done by at least three financial institutions:

i. Issuer Bank

The consumer's card issuer bank, in other words the bank that issued the consumer with the card. This bank determines the level of any fees or any other charges their customer views on his bank statement (Akers, Golter, Lamm, & Solt, 2005).

ii. Acquirer Bank

This is the merchant banks. These kind of banks process card payments on behalf of their clients (merchants). The merchants normally pay an agreed fee to the bank by allowing a small percentage deduction from the transaction amount. Example is where a consumer makes a payment of $100 using a card, the acquiring bank pays the merchant $100 minus a percentage agreed fee (Akers, Golter, Lamm, & Solt, 2005).

iii. The Card Network Association

These are the intermediaries between the two acquirer and the issuer bank. They set and govern the rules of the payment transactions. The institutions include Discover, Visa, MasterCard, Discover among others (Akers, Golter, Lamm, & Solt, 2005).

In an open card payment network, brand card network association such as Visa and MasterCard allow other banks to participate in association. This builds and makes maintenance of the infrastructure easier due to the sharing of switches and lines used to route payment transaction data between the issuing and acquiring banks. In a closed card payment network the card issuer can also be the acquirer. This reduces the number of intermediaries and also the fees charged. Example is Discover and American Express (Hunt , 2003).

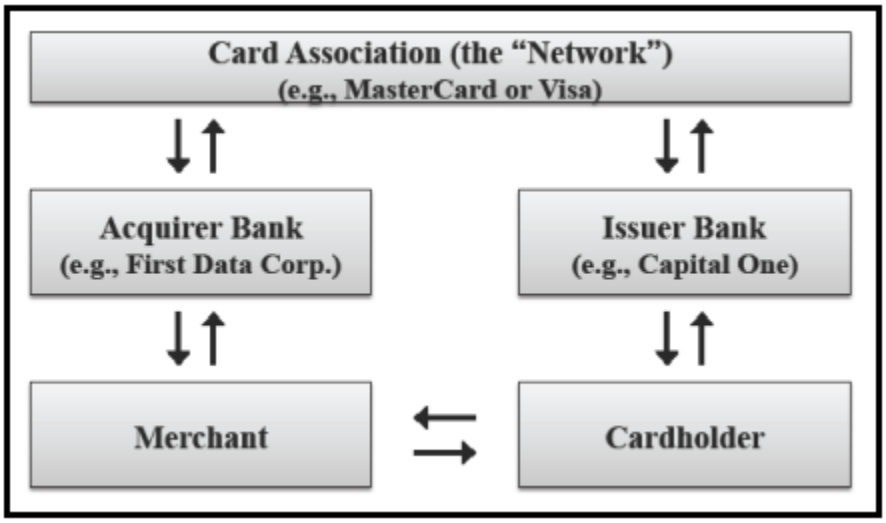


Figure 2.1: Financial Card Network Structure (Levitin, 2011).

2.5 Financial Card Payment Transaction Flow

In a financial card payment transaction the consumer first transfers his card information to the merchant. The transfer can be done by: sending a written form of details as from the order, transferring the information physically via an impression made by an imprinter, sending via radio frequency chip, sending electronically via magnetic swipe or sending electronically via a web. Upon receiving this information, the merchant relays it to the card network for authorisation, capture then settlement. The card information is first verified then the issuer approves the transaction. After the authorisation the amount is transferred from the issuer's bank to the acquirer's bank. This transfer is accounted at the network card association which is the clearance house. The acquirer bank receives the money from the issuer after the clearance, the amount received is less the interchange and network fees. Finally the amount is credited in the merchants account less the merchant discount fee (Levitin, 2011).

2.6 Overview of Financial Card Fraud

Consumer spending behaviours rapid evolvement and merchants widely accepting cards as one of the most convenient ways of payment has drove the world's market for card payment. The wide usage of financial cards replaced the use of paper cheques as a means of paying goods and services. This adoption has made the world to become a paperless and cashless society. Despite this extensive uptake, financial card fraud has become a major drawback (Zareapoora & Shamsolmoal, 2015).

Financial card fraud is when a person uses another person's payment card for his personal reasons when both the card owner and card issuer are not aware of the usage. Furthermore, the person using the card has no intention of neither notifying the card owner or the issuer nor repaying the card amount spent (Levitin, 2011).

Card payment fraud has existed since the introduction of payment cards. As the card payment market increased the card fraud level has increased as well. Every passing year card fraud is costing billions and the figure continues to rise per subsequent year (Sakharova, 2012). According to SAP Annual Report (2016), indicates that card fraud costs the United States payment card industry about 8.6 billion dollars in a year. The report further adds that numbers are speculated to rise in each year due to the volatile nature of the fraud. In addition to the monetary losses, payment card fraud also contributed to loss of consumer confidence in the usage of card payment system thus tarnishing card issuer's brand name and reputation (Sakharova, 2012). Visa Annual Report (2016) indicates that an increase in illegal and fraudulent card events could lead to the company's reputation damage and reduced usage of the visa cards.

Merchants accepting card payments are also at a risk of card fraud mower than the card issuers. This happens when the consumer claim that their fraudulent charge be reversed, the merchant ends up losing the product in sale and pay for chargeback fees because of the fear of losing his reputation and risk of his merchant account closure (Hayashi, Markiewicz, & Sullivan, 2016). This is even worse when the merchant uses an online shop or from merchant website. In a physical scenario the merchant is able to do physical verifications such as a signature check, photo verification and much more while in an online shop is not possible to do any physical check or detect any anomaly. This increases the card payment over the Internet (Hayashi, Markiewicz, & Sullivan, 2016). A

survey report European Payment Council (2017) shows that Internet card fraud is 15 times higher. In the following sub sections we will review the card fraud techniques and their impacts in deeper.

2.7 Techniques Used in Card Fraud

Fraudsters execute payment card fraud in many ways. With the technological advancements and changes, technological fraudsters improve and come up with advanced ways of carrying out their fraudulent activities (European Payment Council, 2017). According to Dara and Gundemoni (2006) there are three broad classifications of fraud namely merchant related, card related and Internet frauds.

2.7.1 Card Related Fraud

Lost or Stolen Cards: This happens when a card is stolen from the legitimate holder of the account or the legitimate card holder loses it. The fraudster then proceeds to use the card for criminal activities. In a fraud scheme report by ROCIC (2015) shows big losses incurred in Atlanta in 2013 where perpetrators who used to steal payments cards at a store were uncovered by FBI.

Application Fraud: This form of fraud happens when an application is falsified so as to get hold of a credit card. This fraud can be committed by: fraudster providing false information about their financial status so as to acquire credit, fraudster illegally assuming the identity of a victim and opening accounts in the victim's name using information which is partially legitimate, or by intercepting cards from the postal service (Dara & Gundemoni, 2006).

Fake or counterfeit cards: in this case, a fraudster innovatively creates counterfeit cards through techniques such as:

i. **Altering the card details:** this is achieved by re-embossing the card or re-encoding the card by use of software applications which encodes the card's magnet stripe data (Paul, Prabhu, & Dua, 2003).

ii. **Creating fake cards:** fraudsters can use sophisticated machines to create fake cards from scratch. However, a lot of effort is required to achieve this since there are many security features designed to deter forgery of cards (Paul, Prabhu, & Dua, 2003).

iii. **Erasure of the magnetic strip:** this done by using powerful electro-magnet to erase the magnetic strip of an illegally acquired card. The details on the card are then tampered with to match those of a valid card that could have been illegally acquired. On swiping the card, it will not work due to the faulty magnetic strip which will then prompt the manual input of the card details into the terminal. This is a risky card fraud method and is less used by fraudsters (Shiv, Ayushi, & Mishra, 2015).

iv. **White plastic:** in this case, the fraudster uses a white plastic (any colour card-size plastic created and encoded with real magnetic stripe data). The card is used for illegal transactions at POS terminals which do not have a card verification or validation requirement (Paul, Prabhu, & Dua, 2003).

v. **Skimming:** in this case, fraudsters use pocket skimming devices which read the card details on the magnet stripe readers of unknowing victims as the victims are waiting for the validation of their transactions. Skimming is very difficult to trace and the victim might remain unaware until they get a bank statements showing transactions they never carried out such as purchases. The card details obtained could also be used to carry out other fraudulent or illegal transactions that do not require the presence of the card (Shiv, Ayushi, & Mishra, 2015).

Account Takeover: in this type of fraud, the fraudster uses illegal means to obtain the personal information of a customer, then takes over the victims account by providing the card number or account number. The fraudster then proceeds masquerade as the real card holder, contacts the issuer of the card and redirects mail to another address. The fraudster then reports to the card issuer that they lost the card and asks for a replacement (Sakharova, 2012).

2.7.2 Merchant Related Fraud

Triangulation: in this case, fraudsters operate from websites. Fraudulent sites appearing to be legitimate sales sites offer goods at discounted rates, and these goods are shipped before payment. A genuine cardholder thinks this is a deal of a lifetime and places online orders, providing information such as their name, valid card details and address on the site. Fraudsters then steal the credit card information and use it to order and purchase goods from other sites (Ogwueleka , 2011).

Merchant collusion: in this fraud, merchant owners or/and employees collude to commit fraud by using the legitimate cardholder or customer personal or accounts information. The merchants or the employees pass this information to fraudsters (Ogwueleka , 2011).

2.7.3 Internet Related Fraud

False or fraudulent merchant sites: this technique is some sort of skimming where fraudsters come up with sites offering very cheap services to customers. Customers have to provide personal information such as name and address, and valid account or credit card information. The criminals then accumulate these information from unsuspecting customers which they use for fraudulent activities (Tripathi & Pavaskar, 2012).

Credit card generation: this is the use of credit card generators which are computer programs, for the generation of valid credit card numbers with valid expiry dates. From one account number, a list of credit card numbers can be generated. The software uses the mathematical Luhn algorithm used by card issuers for the generation of valid combinations of credit card numbers. The fraudsters can generate as many cards as they wish in any format (Ngai, Hu, & Yijun, 2011).

Site cloning: this is another skimming technique where fraudsters clone or spoof order placing pages or entire sites with the aim to get unsuspecting customers' credit card information. The customer does not suspect anything and will receive transaction receipts just as they would from the real company, while the fraudsters gain access to all information needed for credit card fraud (Tripathi & Pavaskar, 2012).

2.8 Impact Caused by Financial Card Fraud

Credit card fraud affects all stakeholders the merchants, acquirers, card holders, card issuers (Spann, 2014). In this sub section we will analyse the impact of credit card fraud on the different players.

2.8.1 Impact on Cardholders

Card holders are the least impacted by credit card fraud due to limited consumer liability when it comes to credit card transactions depending on the country's legislation and consumer protection policies for covering losses from credit card frauds. Card holders just need to report the suspicious

charges and transactions to their issuing bank, which investigates with the merchant and acquirer and then proceeds to process chargeback for the amount disputed (Bhattacharya & West, 2016).

2.8.2 Impact on Merchants

These are the party most affected by credit card fraud, especially in card-not-present transactions since they accept full liability for the losses. A credit card charge dispute by a legitimate card holder leads to a chargeback by the issuing bank to the merchant through the acquirer for the transaction reversal. Lack of physical evidence such as delivery signature challenging the customer dispute places the cost of the fraudulent transaction on the merchant. Thus, credit card frauds are costs the merchants the cost of goods sold, shipping costs, merchant bank fees, loss of or tarnishing of reputation, administrative costs and card association fees (Kosemani, Aghili, & Zavar, 2016).

2.8.3 Impact on Banks (Issuers and Acquirers)

Sometimes it is possible that the card issuers or acquirers bear the cost of the fraud depending on scheme rules. Indirect costs such as chargeback costs also befall the issuer/acquirer. Manpower and administrative costs are also incurred by the issuers and acquirers. Huge investments in form of sophisticated IT systems have to be made by the banks to detect and possibly prevent fraudulent activities (Bhattacharya & West, 2016).

2.9 Techniques Used to Prevent and Manage Financial Card Fraud

As the technological advancement has enabled sophisticated methods for accessing credit card information for fraudsters, it has also enabled means for detection and prevention of fraudulent transactions by merchants and banks (West & Bhattacharya, 2015). These fraud detection techniques allow the performance of highly sophisticated and automated screenings of transactions and flagging any suspicious transactions. These techniques are not sufficient to eliminate fraud by themselves but provide incremental values when it comes to fraud detection. The best practice for fraud prevention implementations utilise several combinations if not all of these techniques (West & Bhattacharya, 2015).This sub section will discuss fraud prevention and management techniques and tools.

2.9.1 Card Verification Methods

Card Verification Method 3 is credit card verification method which consists of a 3 or 4 digit numeric code embossed on the card, but not on the magnetic stripe. This numeric code can be requested by the merchant for card-not-present transactions for verification. CVM aims to ensure that the transacting individual possesses the actual physical card, since the numeric code cannot be skimmed from the magnetic stripe or copied from receipts. CVM thus protects the merchants from transactions carried out in absence of the actual physical card. However it does not protect the merchant from transactions where the fraudster has places transactions on the physical cards which are stolen. Fraudsters can also cope the CVM code when they temporarily possess the card (Balasubramanian & Sivakumar, 2015).

2.9.2 System for Address Verification

This is a technique which is applied in card-not-present situations. The first few digits of the ZIP code information and street address for the purchase billing/delivery are matched to the corresponding on record information held by the card issuers by an AVS. The merchant receives a code which represents a match level between the two addresses. When it comes to international transactions, AVS becomes of not much use (Bahnsen, Aouada, & Stojanovic, 2015).

2.9.3 Manual Review

In this technique, every transaction is manually reviewed for any signs of fraudulent activities. The exercise involves very high levels of human intervention and can thus prove to be time consuming and very expensive. It might also not be able to detect some prevalent fraudulent patterns such as using one credit card multiple times in multiple different locations whether websites or physical location in a short time span (Bahnsen, Aouada, & Stojanovic, 2015).

2.9.4 Fraudulent Merchants

Credit card providers such as Visa and MasterCard are known to publish a list of merchants known to have been involved in transaction that could be deemed fraudulent in the past. The list from MasterCard is called MATCH while that from Visa is called NMAS. These lists provide very useful information that could prevent recruitment of merchants know to have partaken in

fraudulent transactions and thus aid greatly in preventing future fraud (Bhattacharya & West, 2016).

2.9.5 Payer Authentication

This is an emerging technology promising to introduce and bring new security levels to the B2C Internet commerce. The service was first implemented by the Visa Payer Authentication VPAS or VbV program which was launched worldwide in 2002 by Visa. In the program, a PIN is associated with a card, and a secure channel for authentication between the consumer and issuing bank. The bank issues the PIN when the card holder enrols their card with the program, and is extensively used for the authorisation of online transactions. The registered card holders are prompted by their issuing bank to provide their password when checking out participating merchants' sites and on verification of the password, the merchant completes the transaction and passes on the verification information to the acquirer (Randhawa, Loo, & Seera, 2018).

2.9.6 Lockout Mechanisms

As discussed in the fraud techniques, card number generators are a technological tool frequently used by fraudsters. Based on the symptoms associated with this technique such as multiple transactions for similar card numbers and large amount of declines, the acquiring banks or merchants can implement preventive mechanisms which are specifically designed for the detection of card number generation attacks (Balasubramanian & Sivakumar, 2015).

2.10 Challenges in Payment Card Fraud Detection

With the rampant and gradually increasing credit card theft, methods to detect and identify fraud in credit card have deemed necessary. Different methods have been created to identify and differentiate between genuine and fake transactions. The different systems in existence have the capacity to make out counterfeit transactions as well as the prospect of occasion of fraud (Sakharova, 2012).

In the manual reporting where an account holder detects a fake banking transaction they report to the bank. The bank then proceeds to take the appropriate steps to curb financial loss from occurring. When fraud is detected quickly and necessary steps taken quickly, users develop trust

and confidence in the bank. This also augments the value of the bank therefore leading to an increase in the profits generated. Any customer needs to feel assured that their bank will preserve their financial data and take quick action in the face of a counterfeit credit card transaction (Spann, 2014).

The increased use of credit cards to make purchases online has however increased the challenge of credit card fraud. When a user registers to make online purchases from a website, the username and password are sent to their email for them to use when accessing the website. During the process of purchase only credit card characteristics are examined if they are right and the user can make the purchase. The email is the only one that is examined and personal details about the credit card holder are not checked during the time of registration. Therefore, they cannot be certain that it is the card owner who has made the purchase. Therefore, fraudsters can generate fake emails and conduct fraud and the administrators realise when the fraud has already taken place or if the original owner sends a complaint (Sakharova, 2012).

Fraudsters are also changing their techniques with time in order to penetrate any new credit card fraud detection system. This poses as a challenge as it makes it difficult for human experts to predict fraud due to its complexity and sophistication. It makes it necessary for increased research on the dynamic behaviour of fraudsters. Moreover, the lack of real data set also poses as a challenge in credit card fraud detection. This is a major challenge because researchers don't have enough information they require to conduct research on credit card fraud. This lack of information is as a result of banks and financial institutions unwillingness to reveal sensitive information regarding their customer transaction data because of reasons of privacy (Sadeghi, 2013).

Millions of credit card transactions are made on a daily basis. Analysing all of these transactions is another challenge since they require techniques that are highly competent due to the enormous transactions (Malini & Pushpa, 2017).

Establishing and identifying the best card fraud evaluation parameter is also a challenge. There are two main measures of fraud detection techniques which are the false positive and false negative rates. The two measures have a relationship which is opposite to each other in that when one reduces the other increases. The data set is also imbalanced making accuracy an unsuitable

technique for credit card fraud detection (Malini & Pushpa, 2017). There is also a vast difference in misclassification costs where the error cost of misclassifying fraudulent events is greater than the error cost of misclassifying genuine activities. Therefore, it is important to consider both the sensibility and precision of each case (Spann, 2014).

2.11 Related User Reporting Systems

There are several systems in different countries created to enable people to report property loss or theft. Examples of such systems include immobilise and UC Davis Police Department Lost and Found Unit.

2.11.1 Immobilise

Immobilise normally used by members of the public and businesses to register their valued possessions or company assets, and exclusive to Immobilise all account holders registered items and ownership details are viewable on the Police national property database. Immobilise helps Police identify the owners of recovered property thousands of times every day (Immobilise.com, 2018).

2.11.2 UC Davis Police Department Lost and Found Unit

UC Davis Police Department Lost and Found Unit is the central repository for lost and found items on the Davis and Medical Centre campuses. If you find a lost item on the Davis or Medical Center campuses, it is your responsibility to turn the item in at the UC Davis Police Department front counter. Police are responsible of finding the item owner and delivery of the item to the owner (Police.ucdavis.edu, 2018).

2.11.3 UCPD Lost and Found

UCPD Lost and Found is the central repository for items lost and found on campus. They use a form to enter information about the Item you've lost. They emphasise that it is helpful if they have your CalNet Directory listing so that they can easily let you know if they have your item in their repository of Lost and Found (Ucpd.berkeley.edu, 2018).

They also recommend people to report to found@berkeley.edu including their details name and contact information, the date their item was lost, the type of item, including the brand, colour and any details that would make it easier to identify the item as theirs (Ucpd.berkeley.edu, 2018).

2.11.4 Conclusion

These systems help a person report theft or loss with ease. To report identity items on immobilise for example, one needs to sign up or login to an immobilise account. They then register the item which is then reported. The application entails steps which one is required to follow to file the report. The system is linked to the police who are then able to search serial numbers of recovered identity property. That way, they are able to take the necessary action. These systems however heavily rely on well-wishers for the return of stolen items. It does not focus on curtailing and curbing of crimes involving the theft of identity items (Miller, 2007).

2.12 Schematic Design

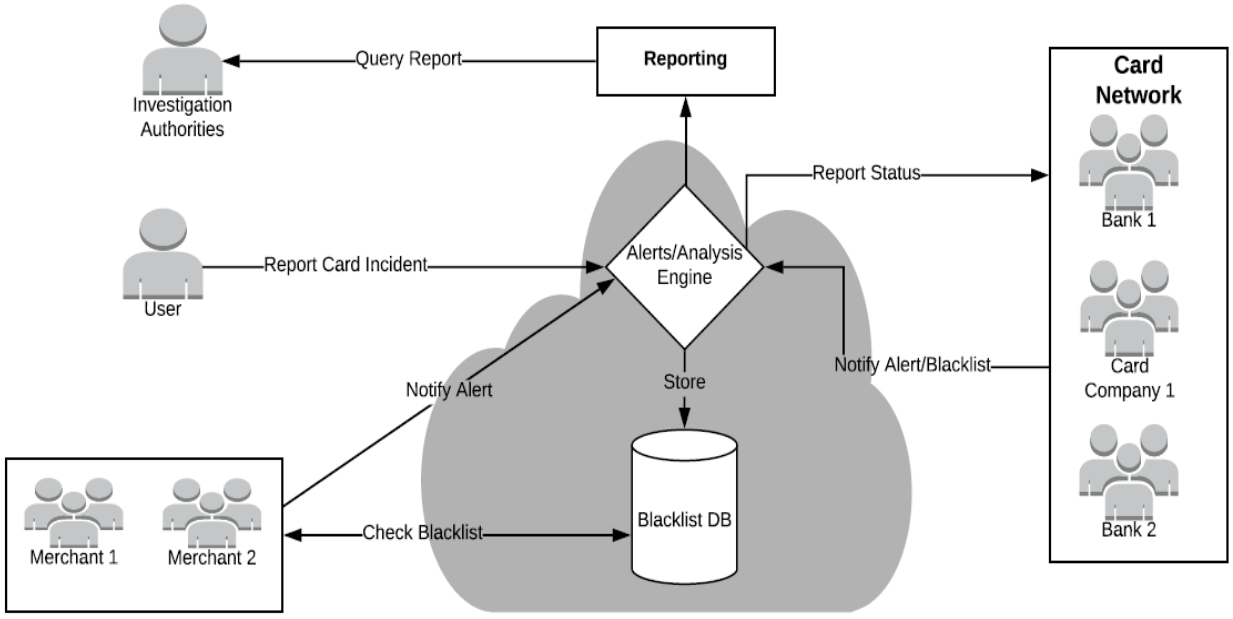


Figure 2.2: Schematic Diagram

In the proposed system the financial card network stakeholders (banks, card industry, individual card holders and merchants) will collaborate to build a blacklist database and send alerts of fraud cases. This collaboration comes in to assist the network. Information from the user and analysis

by the different merchants systems, different banks systems will be shared across the platform. This will significantly reduce the card fraud.

Banking sector, merchant and card industries all have different systems in place to prevent cards fraud. Bringing in the collaborative nature of the system ensured when one stakeholder learns of a fraudulent financial digital identity using his systems, all the other stakeholders are aware of the rogue card identity, thus lesser surface of fraud. The system indirectly assists in system capabilities and resources sharing thus enhancing more security and assurance in the card industry.

2.13 Conclusion

In the current era people should be careful and cautious in protecting their identity items to prevent them from identity theft. Nobody is sure that he will not fall in the list of millions of identity fraud victims (Hedayati, 2012). Criminals are utilising technological advancement to carry out various credit card fraud activities such generating card numbers, merchant collusion and skimming. However, the changing, improving and advancing technology also provides mechanisms for preventing and dealing with this credit card fraud (Papaa & Jamei, 2015). These frauds can be dealt with using various methods such as address verification, manual reviews and payer authentication. No one method is sufficient to prevent the fraud, and a combination of many means leads to better prevention rates and hence less occurrence of the credit card frauds. An optimally balanced total cost of fraud can be reached through the collaboration of merchants, card issuers, card acquirers and card holders (Tripathi & Pavaskar, 2012).

Chapter 3: Research Methodology

3.1 Introduction

This chapter covers the methodology used to achieve this dissertation's objective. It discusses each methodology step detailing all activities and processes involved in order to achieve the proposed system.

3.2 Research Design

The main aim of research design is to help in collection of relevant research materials that will help the researcher in addressing the research objectives, problem statement and testing the hypothesis (Chilisa, 2012). This section includes how data collection was done, the modes of data collection used, how they were applied and how data was analysed.

Literature review was conducted through a systematic review of reports, journals, articles, and books. These materials were selected based on the research title keywords. The identified relevant literature was used to investigate the fraudulent acts caused due to lost or stolen financial cards and helped in the review of methods used to prevent and investigate fraudulent usage of lost financial cards. A controlled assessment study was conducted during the review of the literature. These assessment study was based on the relevance of the literature to the research objectives. This helped to assess the quality of the literature in accordance with the keywords and the research questions which were being examined. Card industry sector financial reports were reviewed to evaluate the current financial card fraud state.

This research, applied incremental delivery where the system's increments were to be delivered for testing and comments to the card industry stakeholders (banks, card association, merchant and individual card holders). The first deliver (version 1.0) was delivered by this dissertation as the key prototype. Incremental delivery is change tolerant and focuses on continuous gathering of correct system requirements (Parsons, 2012). This will enhance a good implementation when integrating with different card industry stakeholder systems. It enhances incremental addition of new stakeholders APIs and allows a smooth transition for future works. Furthermore, the increments helped in identifying missed system requirements which helped to improve the system's functionalities.

3.3 Software Development Methodology

Agile methodology was adopted for the software development. Agile software methodology is an incremental and iterative methodology that uses incremental and rapid sprints in development. These cycles focus on improving the system, where small incremental releases are released with each release builds on the previous functionality (Kong, 2007). The results of each sprint were tested thoroughly focusing on the improvement of the system's functionality.

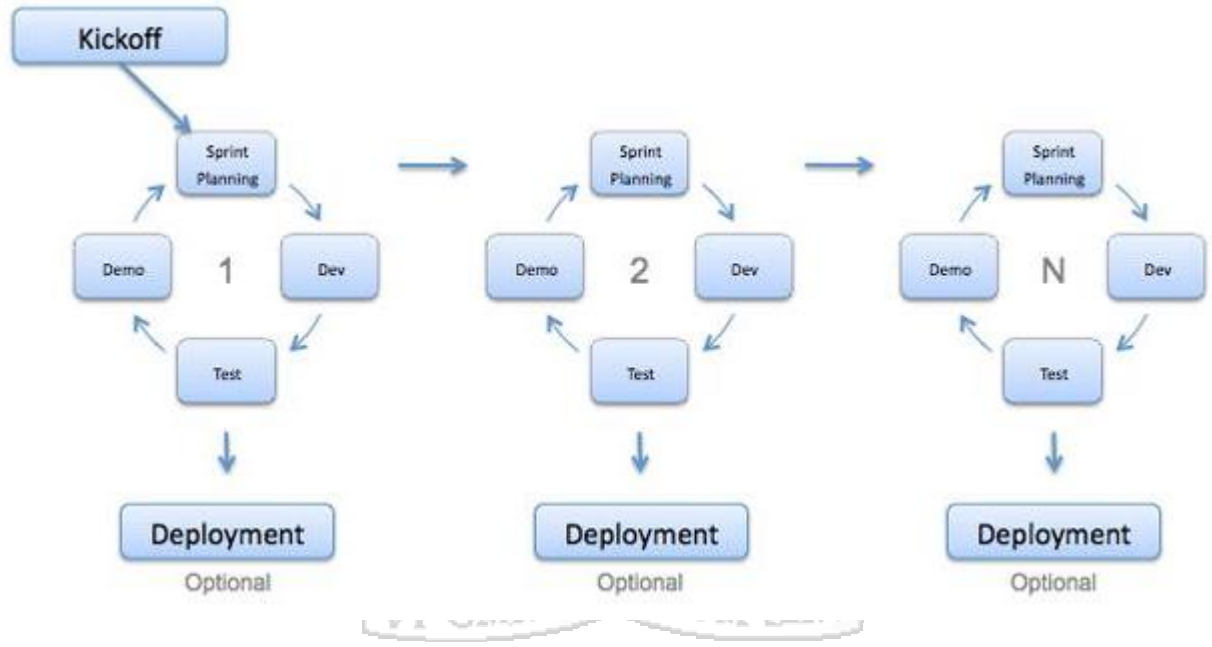


Figure 3.1: Agile Methodology Splints (Half, 2014)

According to Kong (2007), each sprint of agile software development life cycle has the following phases, they include: planning, requirement analysis, design, building, testing and deployment.

3.3.1 Planning Phase

This is the initial phase of the methodology. Its objective was to give planning procedures that will facilitate the development process. This entails planning of all activities and processes involved to deliver the solution. This phase helped in identifying the resources needed from different stakeholders (banks, card industry, individual card holders and merchants) so as to come up with an effective system to prevent financial card identity fraud.

3.3.2 Requirement Analysis Phase

This is the second phase of agile SDLC. It involved analysing the system requirements. Here the researcher needs to document and understand the whole process. Structured analysis was carried out on the data gathered from the reviews to determine models. Use cases were developed based on the data model analysis.

The analysis helped in determining which parameters and where they were relevant to be applied. The availability and knowledge of this information was necessary before any development of code. Therefore, data was collected from relevant literature reviews of existing solutions to determine the gaps that were not covered, this helped to create system test cases to evaluate and validate the solution.

3.3.2.1 Data Collection Process

Data collection was done to help investigate the fraud crimes caused due to lost or compromised financial cards and review of methods used to prevent and investigate fraudulent usage of compromised financial cards so as to implement a proper way of combating this kind of fraud. Financial card fraud incident reports from leading banks and card brands were as the main reference.

i. Card Fraud Incident Reports Review

When reviewing the financial card fraud acts, crimes caused by these acts and techniques used to combat these kind of acts, leading card industry companies, leading merchant and banks yearly fraud reports were reviewed to get the trend and current status of card fraud. Various documents with relevant information were reviewed to provide an in-depth knowledge on what current and earlier developments were done in this line of research. The literature review was conducted on as a systematic review of financial card industry fraud reports, journals, articles, and other relevant books.

3.3.2.2 Data Analysis and Functional Modelling

Key fraudulent financial identity items and key crime targets were identified, analysed and classified according to their impact. They were well prioritised with their level of impact. This information helped to reveal what kind of stakeholders to prioritise, which techniques, which parameters to apply in order to have a functional system.

3.3.3 Designing Phase

The design phase occurs after proper comprehending the system's requirements analysis. Use case diagrams, wireframes, entity relation diagrams and sequence diagram to conduct an initial system design were developed. This aided in determining its appearance and operation scheme. This was followed by a detailed and formal system design that meets all the relevant requirements.

3.3.4 Building Phase

At this stage, the system coding was done based on the designs produced by the previous phase. Entity relation diagrams were be used in designing the database and defining the relation of different actors to reported identity data in order to develop a fine-grained access control mechanism in the access API. Wireframes were used in coming up with system interfaces and overall system functionality.

3.3.4.1 Incremental Development

Development of the system involved the following:

i. APIs exposed to the different actors were developed using Restful web services.
ii. Apache web server was set up in the cloud which hosted the web services.
iii. PostgreSQL database that was used to maintain the records of the reported incidents and investigative responses from the stakeholders.
iv. Netbeans IDE was used for development and postman was used to test the rest web services.
v. Postman was used to validate input and output of the APIs

3.3.5 Testing and Deployment Phase

After a successful completion of a sprint, testing of the resultant release followed. This was done aiming at checking whether the systems objectives are met. Sample financial card fraud incidents and possible responses from the relevant card industry stakeholders were loaded into the system for testing purposes. Test cases developed from the documented requirements were used in this dissertation. End to end tests of the test cases were done. The tests were mainly based on system usability and system functionality.

i. Functional testing

Functional testing was done for the entire system to ensure that the system's functions were functioning properly and as expected. The system was tested to see that the reported card data reached the stakeholder for blacklisting or tracking, appropriate responses and triggers were received for fraud investigation. Postman was used as the API input output test tool.

ii. Usability testing

Usability tests were done after the system is fully functional. This was done to test the user friendliness of the system. This is mainly to ensure that a case would be filed, sent to the relevant stakeholder, informative information would be received ensuring that the compromised card would not be fraudulently used.

3.4 System Validation

The system was to be validated by evaluating the success rate of the test cases developed during requirement analysis phase. Different stakeholders APIs were tested, a financial card incident was reported, sent for blacklist to the relevant stakeholder and a tracking trace was set to send trigger in case of any usage of the card. This helped us validate that the system can reduce and assists in investigation of fraud caused by compromised financial cards.

3.5 Ethical Measures

To observe and ensure an ethical code of conduct the research was compliant with PCI (Payment Card Industry) data security standards in storing and transmitting cardholder data (PCI, 2018). This will include but not limited to; installation and maintain a firewall configuration to protect cardholder data, encryption in transmission of cardholder data across open and public networks, use and regularly update anti-virus software or programs, restricting access to cardholder data by business need-to-know, assigning a unique ID to each person with system access, restricting physical access to cardholder data, track and monitoring all access to network resources and cardholder data, regularly testing of security systems and processes and maintaining a policy that addresses information security for employees and contractors

3.6 Conclusion

This chapter has highlighted the processes and methods used to collect facts and data as well as answering the asked research questions. It goes further to explain the validation tests done, the security and ethical measure taken.

Chapter 4: System Design and Architecture

4.1 Introduction

A real time reporting system prototype was developed to demonstrate an implementation that will help in reporting and preventing fraud of the lost or compromised payment cards. This chapter presents the system architecture and the components that were used to come up with the proposed solution. Interaction diagrams helped to demonstrate the interaction between users and the system and to show the flow of data from one point to another.

4.2 System Architecture

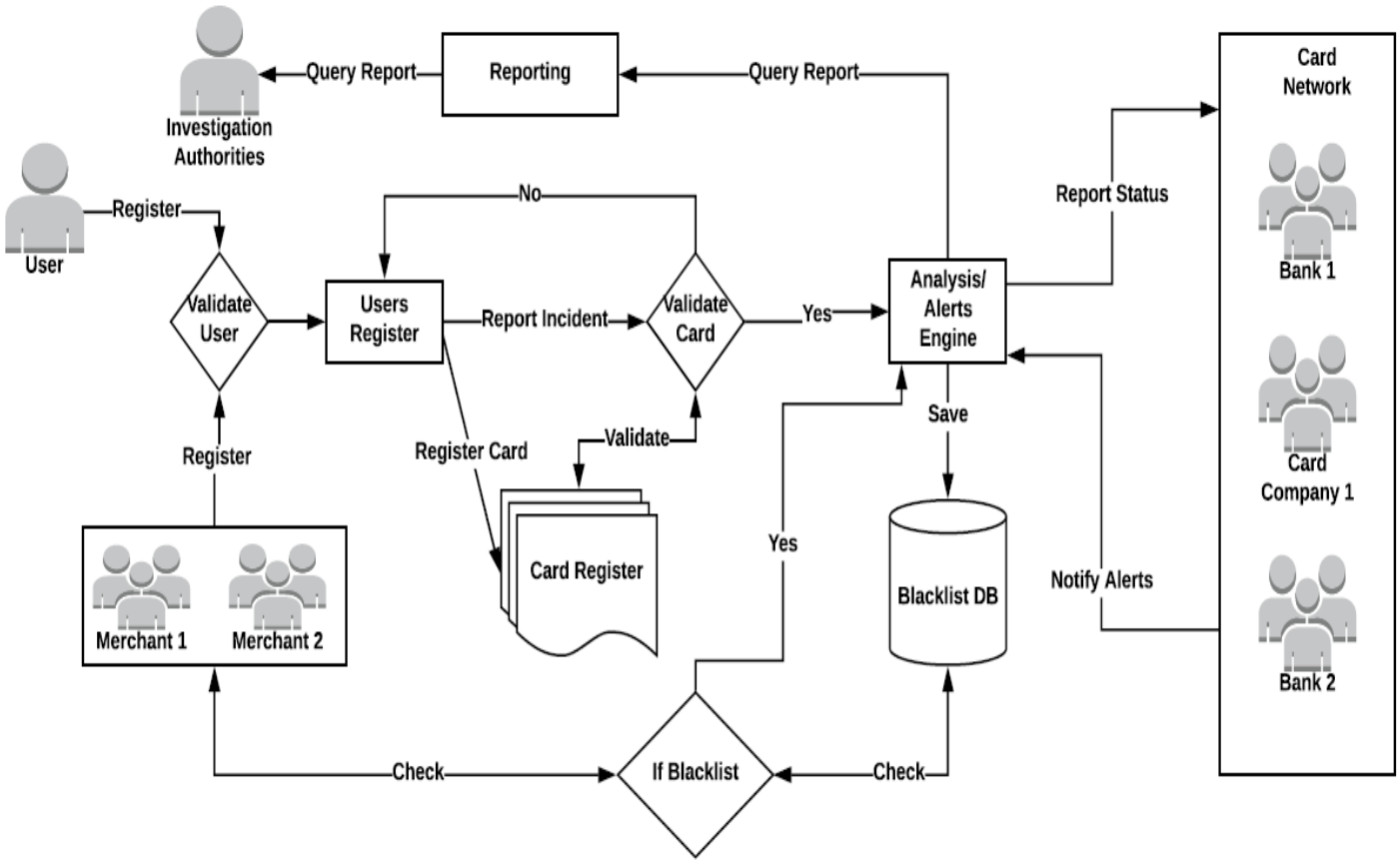


Figure 4.1: Shows the Proposed System Model

4.2.1 System Components

The proposed system comprise of a user register, card register, analysis engine, a blacklist database and a reporting module. The system stakeholder or actors include banks, card industry, individual card owners and merchants. The components are as discussed below:

1. User Register

The user register comprise of a list of vetted, verified and validated users who can access the system. This are the users who can be able to query blacklist database, to push alerts to the system and to report an incident of a payment card identity loss or theft or compromise. The user's details are well captured, thoroughly vetted and validate against his or her documents to allow high level of legitimacy. To ensure a high level of legitimacy individual owners are registered by their issuer bank at the time of card issuance. After validation a successful user account is created and issued with login credentials.

2. Card Register

This is a list of payment cards registered in the system. Authorised users can register their card details in their account for close monitoring and ensure ease in incident reporting. When a lost or stolen card is already registered in your individual account you will be able to report right away with any validations thus reducing the crime window. These cards are vetted and validated to be owned by the user before they are put in the users account. To ensure legitimate owner definition card ownership is linked to the individual owner by the issuer in time of issuance.

3. Analysis Engine

This engine analyses information from the different system stakeholders. It analyses: incidents reported by all the system users, it analysis alerts sent by merchants and the entire card network association. It does the categorisation of these information and prepares it for reporting.

4. Reporting Module

This is a module that tables payment card information about incidents and alerts as categorised by the analysis engine. It presents information rich and well-structured reports to assist in investigations and decision making.

Banking sector, merchant and card industries all have different systems in place to prevent cards fraud. Bringing in the collaborative nature of the system ensured when one stakeholder learns of a fraudulent financial digital identity using his systems, all the other stakeholders are aware of the rogue card identity, thus lesser surface of fraud. The system indirectly assists in system capabilities and resources sharing thus enhancing more security in the card industry.

4.3 System Design

In this section we focus on the design structure of the solution. It shows the system modules, how they are inter-related and how they work together to achieve our desired objective. The designs are the use case diagram, system sequence diagram and the entity relation diagram. The use case diagrams are used to show the reaction of the system based on the action events given by the stakeholders. The sequence diagrams are used to illustrate the sequence of the events in the system and show the flow of information among the different entities of the system.

4.3.1 Use Case Diagram

This Unified Modelling Language tool was used to map and identify system actors and their use cases in an iterative unified process that links each system actor with particular action in the system as shown in Figure 4.2.

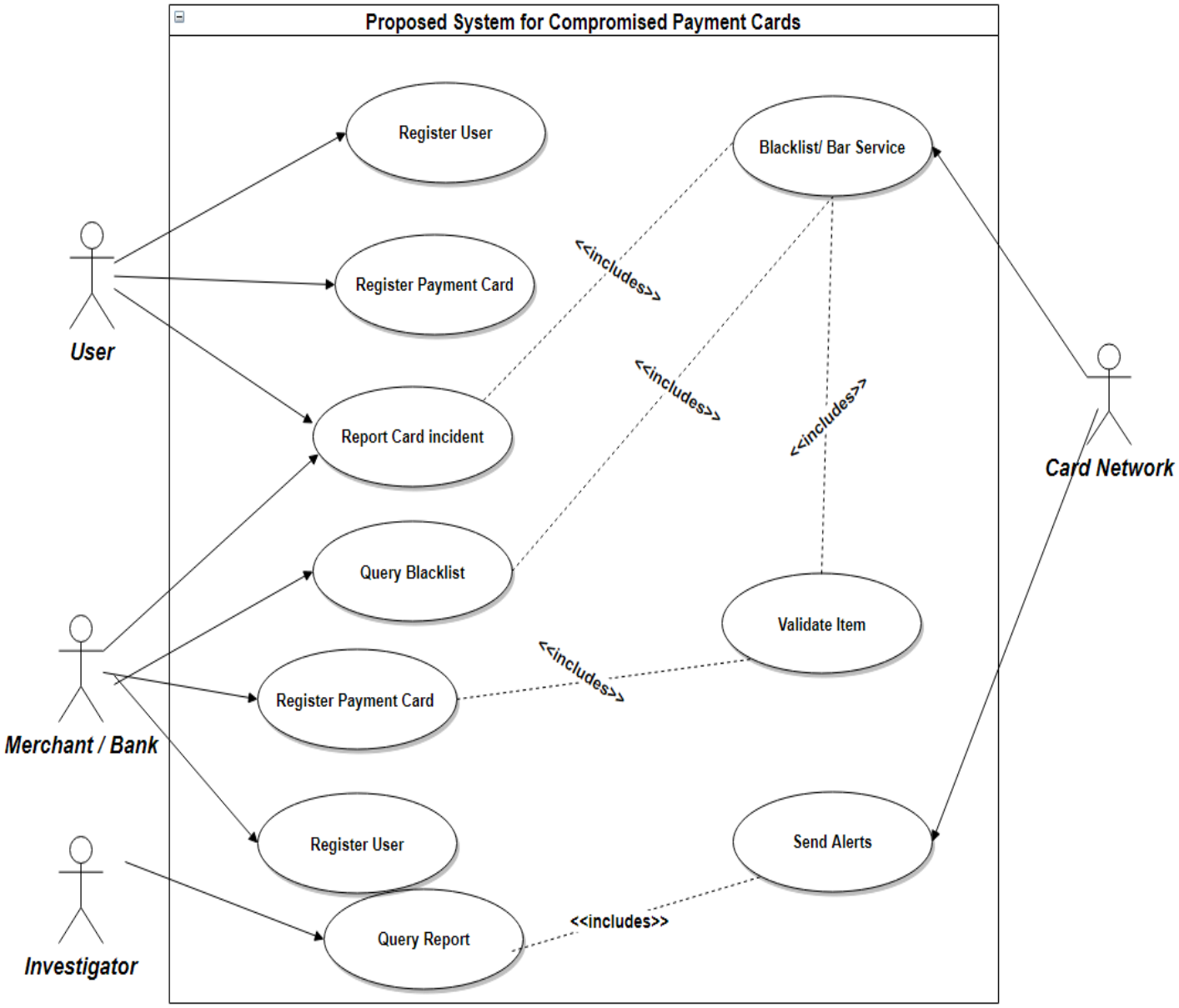


Figure 4.2: Use Case Diagram of the Proposed System

4.3.1.1 Use Case Diagram Description

The above use case diagram describes various use cases showing the key parties in the use case. Below we will elaborate the use cases showing their pre-conditions (the conditions that should be fulfilled before the operation begin), post-conditions (the conditions that will be achieved at the end of an operation) and their main success scenario of the system. Table 4.1 describes the user registration process which is followed by the payment card registration process as described by Table 4.2. Table 4.3 describes how a compromised card incident will be reported. Table 4.4

describes how the stakeholders will access the blacklist database. Table 4.5 describes how a stakeholder can log alerts about fraudulent payment details. Table 4.6 describes how to query system investigative or statistical reports.

Table 4.1: Register User Use Case Description

Title:	Register User
Description:	System users individuals and entire card network stakeholders are registered here
Primary Actor:	Users: Card Issuers ,Merchants and Card owners
Preconditions:	User has no valid credentials or failed login attempt.
Post-conditions:	User is registered into the system.
Main Success Scenario:	1. Privileged user selects “Register” from the main menu. 2. User fills in their details. 3. User clicks “Submit”. 4. System registers the user and displays a success message.
Extensions:	3a. Invalid input. --3a1. System displays error message saying invalid registration. --3a2. User either backs out of this use case or provides valid details and tries again 3b. Existing user. --3b1. System displays error message saying the user exists. --3b2. User backs out and goes to the login use case.
Frequency of Use:	Once

Table 4.2: Register Payment Card Use Case Description

Title:	Register Payment Card
Description:	Registers payment card and links it to owner's account
Primary Actor:	Users: Card Issuers ,Merchants and Card owners
Preconditions:	The user has an account.
Post-conditions:	Payment card is registered in to owner's account
Main Success Scenario:	1. Privileged user selects "Register Card" from the main menu. 2. User fills in the card details. 3. User links the card to its owners account. 4. User clicks "Save Key" 5. System saves the card and displays a success message.
Extensions:	3a. Invalid input. --3a1. System displays error message saying invalid registration. --3a2. User either backs out of this use case or provides valid details and tries again 3b. Existing card. --3b1. System displays error message saying the card exists. --3b2. User backs out and goes to the login use case.
Frequency of Use:	Once

Table 4.3: Report Card Incident Use Case Description

Title:	Report Card Incident
Description:	Card owners report incidents of compromise, lose or theft of their payment cards.
Primary Actor:	Users: Card owners
Preconditions:	Card owner is registered and has a payment card.

Post-conditions:	Card is flagged in blacklist
Main Success Scenario:	1. User selects “Report Incident” from the Incident menu. 2. User selects the compromised card 3. User fills the incident details in the form 4. User clicks “Submit”. 5. System displays a success message.
Frequency of Use:	Many

Table 4.4: Query Blacklist Use Case Description

Title:	Query Blacklist
Description:	Users query card blacklist database
Primary Actor:	Users: Card Issuers, Merchants
Preconditions:	Registered user with privileged access to API
Post-conditions:	Response status of blacklist or not blacklist
Main Success Scenario:	1. User access query API 2. Supplies card details 3. System gives response of blacklist or not blacklist.
Extensions:	3. Invalid request. 1. System displays error message saying invalid request. 2. User either backs out of this use case or provides a valid request and tries again
Frequency of Use:	Many

Table 4.5: Send Alert Use Case Description

Title:	Send Alert
Description:	Channel to receives alerts of reported payment cards and other card payment fraudulent informations collected by stakeholders
Primary Actor:	Users
Preconditions:	Registered user with privileged access to API
Post-conditions:	Response status of alert logged successfully
Main Success Scenario:	1. User access query API 2. Supplies alert information 3. System gives response of success.
Frequency of Use:	Many

Table 4.6: Query Report Use Case Description

Title:	Query Report
Description:	Users access status, statistical and investigative reports here
Primary Actor:	Users
Preconditions:	User is registered and has access.
Post-conditions:	User will get the report.
Main Success Scenario:	1. User selects “Reports” from the main menu. 2. User selects the report. 3. System displays the report.
Frequency of Use:	Many

4.3.2 Sequence Diagram

Sequence diagrams were used to illustrate the association between objects in the successive requests. Here the diagrams show the collaborations between the entities in the system, this is well illustrated by the messages passed from one entity to the next and the response denoted in the opposite direction as shown in Figure 4.4. The Figure shows how events take place in respect to the system users. A registered user can report a card compromise incident which will result to blacklisting or suspending the card. Merchants can query the blacklist database to check whether the card in use is suspended. Card network stakeholders can send alerts about the blacklisted cards or any other fraudulent card payment activity. Investigators can query reports or alerts concerning a reported incident.

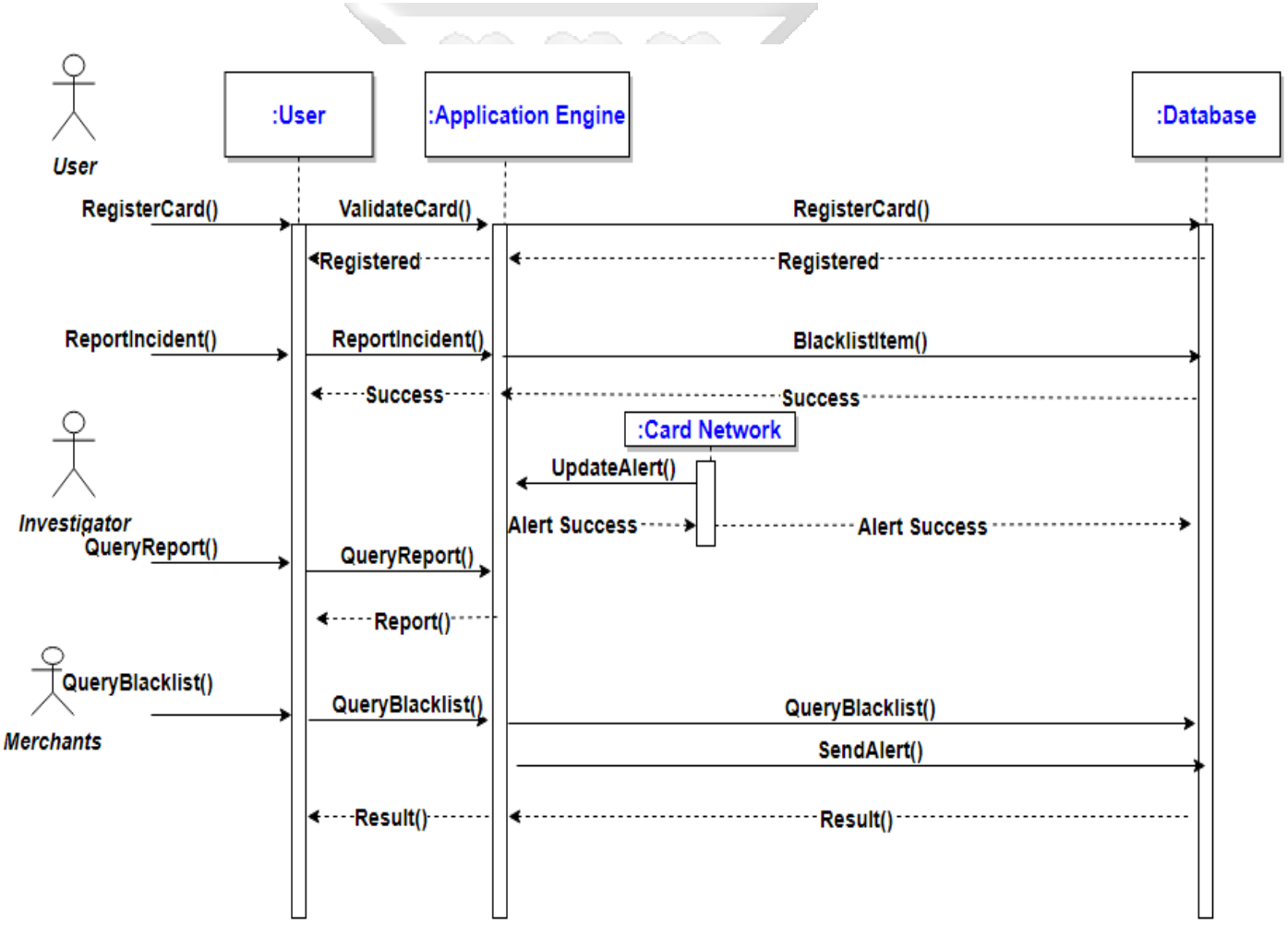


Figure 4.3: Sequence Diagram of the Proposed System

4.3.3 Entity Relation Diagram

The entity relation diagram shows all the entities of the system and how they are related to each other. The entity diagram for the proposed system is as shown in Figure 4.4

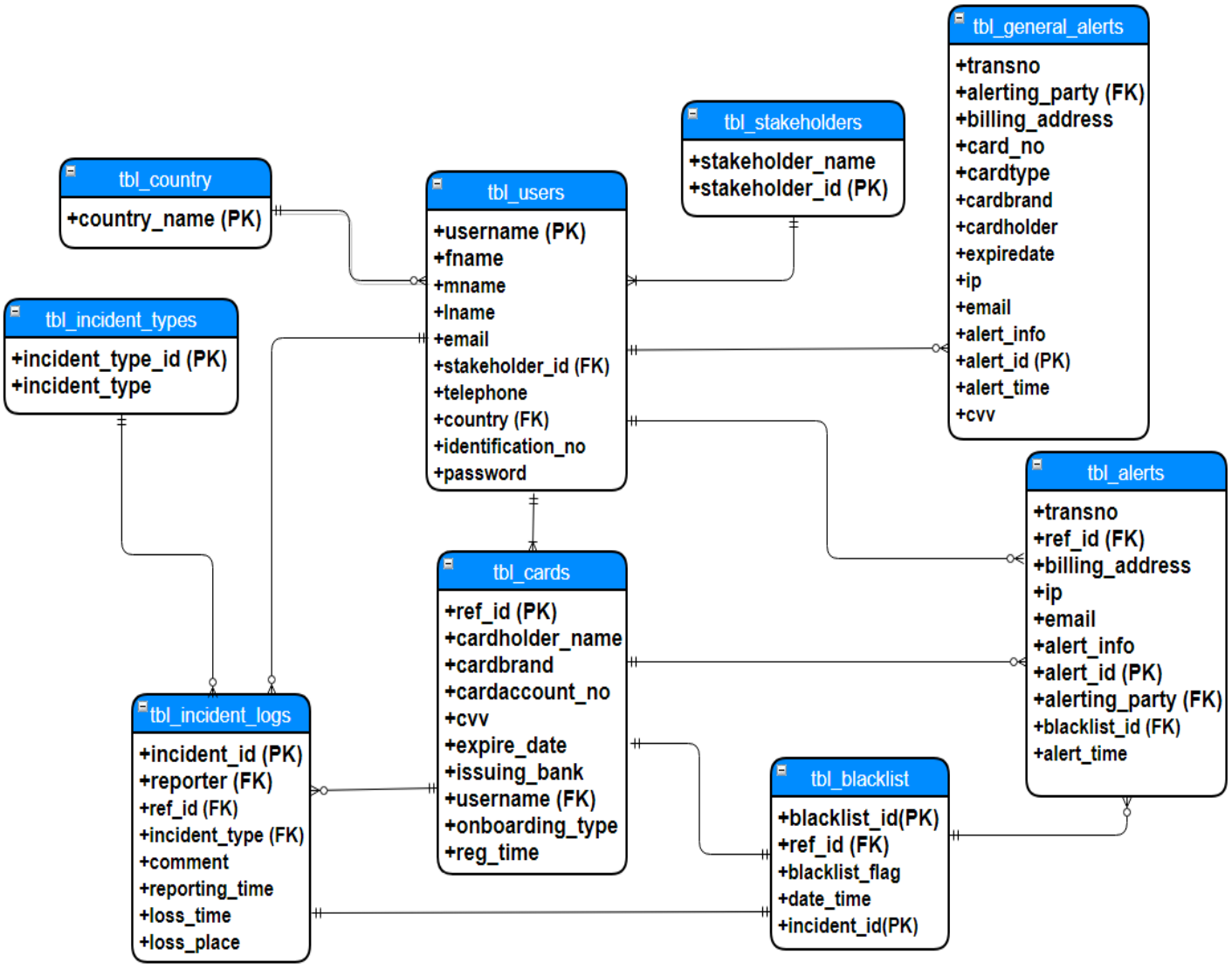


Figure 4.4: Entity Relation Diagram of the Proposed System

Table 4.7 illustrates the overview of the entities of the database and their description.

Table 4.7: Database Tables Overview

Table Name	Description
tbl_alert_params	It holds categorisation parameters for alerts
tbl_alerts	It logs specific card alerts
tbl_blacklist	It stores the status of the card (blacklist or not)
tbl_cards	It stores card details
tbl_general_alerts	It stores any other alerts not associated to a specific card
tbl_incident_logs	It logs all the card incidents reported
tbl_incident_types	It holds categorisation parameters for incidents
tbl_stakeholders	It categorises the stakeholders
tbl_users	It stores system users

4.3.4 Database Schema

The database schema provides detailed description of the database, detailing the entities attributes, primary keys, foreign keys. The tables in this section represent the core tables for the system functionalities

Table 4.8: Users Table

Table Name: tbl_users		
Column Name	**Data Type**	**Index**
username	character varying(15)	PRIMARY KEY
fname	character varying(15)	
mname	character varying(15)	
lname	character varying(15)	
email	character varying(100)	
stakeholder_id	integer	FOREIGN KEY

telephone	character varying(15)	
country	character varying(50)	
identification_no	character varying(100)	

Table 4.9: Incidents Table

Table Name: tbl_incident_logs		
Column Name	**Data Type**	**Index**
incident_id	integer	PRIMARY KEY
reporter	character varying(15)	FOREIGN KEY
ref_id	integer	FOREIGN KEY
incident_type	integer	FOREIGN KEY
place_of_incident	character varying(200)	
incident_time	timestamp	
reporting_time	timestamp	

Table 4.10: Alerts Table

Table Name: tbl_alerts		
Column Name	**Data Type**	**Index**
transno	integer	
ref_id	integer	FOREIGN KEY
param_id	integer	FOREIGN KEY
Param_details	character varying(200)	
alert_id	integer	PRIMARY KEY
alerting_party	character varying(15)	FOREIGN KEY

blacklist_id	integer	FOREIGN KEY
alert_info	text	
alert_time	timestamp	

Table 4.11: General Alerts Table

Table Name: tbl_general_alerts		
Column Name	**Data Type**	**Index**
transno	integer	
param_id	integer	FOREIGN KEY
Param_details	character varying(200)	
alert_id	integer	PRIMARY KEY
alerting_party	character varying(15)	FOREIGN KEY
alert_info	text	
alert_time	timestamp	

Table 4.12: Blacklist Table

Table Name: tbl_blacklist		
Column Name	**Data Type**	**Index**
blacklist_id	integer	PRIMARY KEY
ref_id	integer	FOREIGN KEY
blacklist_flag	boolean	
date_time	timestamp	
incident_id	integer	FOREIGN KEY

Table 4.13: Incident Types Table

Table Name: tbl_incident_types		
Column Name	**Data Type**	**Index**
incident_type_id	integer	PRIMARY KEY
incident_type	character varying(100)	

Table 4.14: Cards Table

Table Name: tbl_cards		
Column Name	**Data Type**	**Index**
ref_id	integer	PRIMARY KEY
cardholder_name	character varying(200)	
cardbrand	character varying(200)	
cardaccount_no	big integer	
cvv	integer	
expiredate	date	
issuing_bank	character varying(200)	
username	character varying(15)	FOREIGN KEY
card_type	character varying(50)	
Onboarding_type	character varying(50)	
registered_by	character varying(15)	FOREIGN KEY
reg_time	timestamp	

Table 4.15: Stakeholders Table

Table Name: tbl_stakeholders		
Column Name	**Data Type**	**Index**
stakeholder_id	integer	PRIMARY KEY
Stakeholder_name	character varying(100)	

Table 4.16: Alert Parameters Table

Table Name: tbl_alert_params		
Column Name	**Data Type**	**Index**
param_id	integer	PRIMARY KEY
param	character varying(200)	

4.3.5 Wireframes

A wireframe is a low-fidelity representation of a system design. Figure 4.5 below shows the main screen, has all the menus for services accessible via the graphical user interface. Other wireframe diagrams can be found at Appendix A. Appendix Figure A.1 shows wireframe for user registration, Appendix Figure A.2 shows wireframe for login page, Appendix Figure A.3 shows wireframe for card registration and Appendix Figure A.4 shows wireframe for reporting incidents.

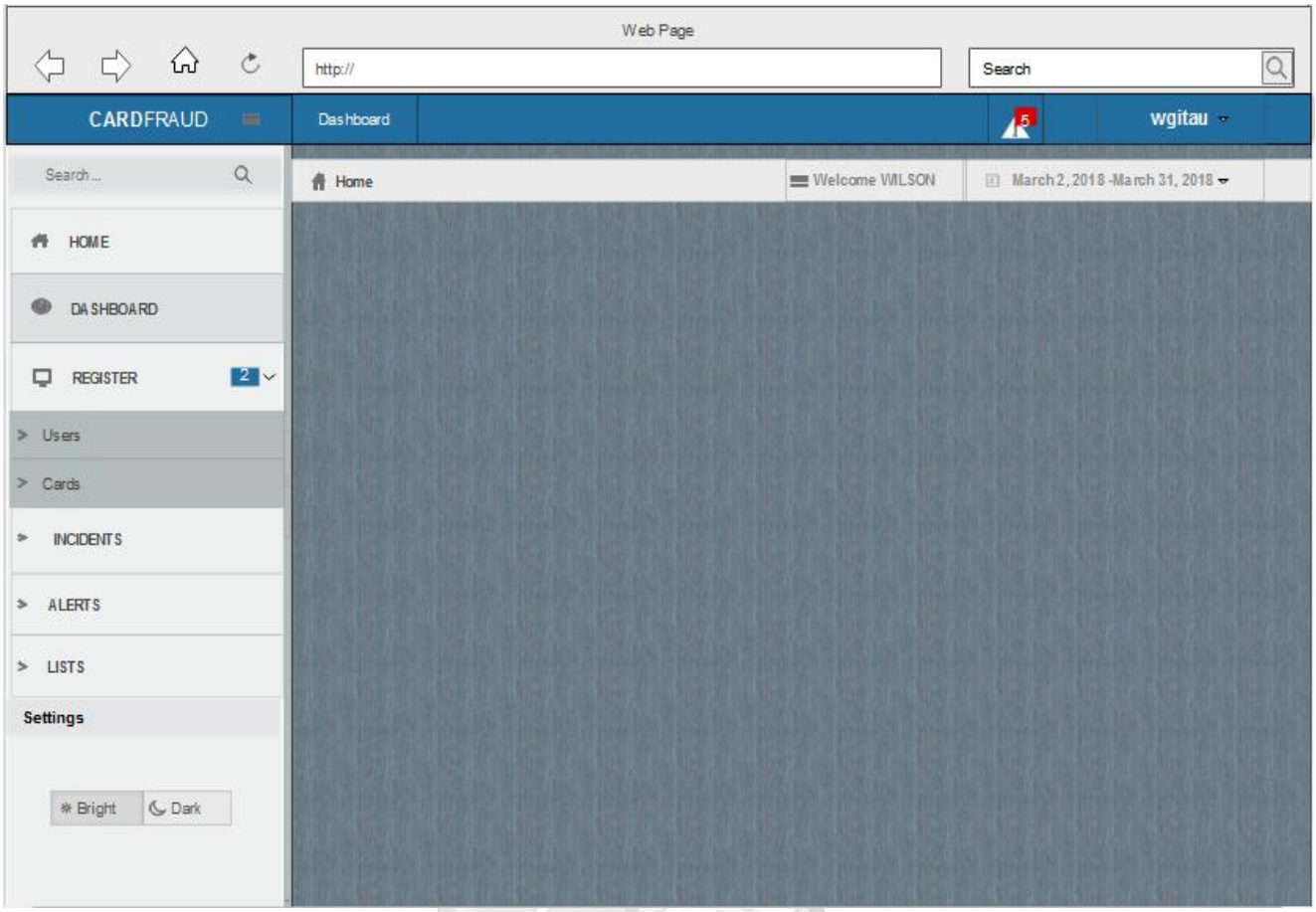


Figure 4.5: Wireframe Showing all the GUI Menus

4.3.6 Application Interfaces

Application Programming Interface is a software intermediary that allows two applications to talk to each other. Our application interface will hold interaction interfaces among the stakeholders. Restful web services will be developed to allow the communication. This subsection explains the shows the inputs and outputs of various services in the system.

4.3.6.1 QueryBlacklist Interface

The QueryBlacklist interface will be used to get the status of the card. The merchants and banks will use it to check the status before completing the transaction. Table 4.17 shows the inputs and outputs of the interface.

Table 4.17: Shows QueryBlacklist Web Service API Parameters

Web Service Name: QueryBlacklist	
Input	**Output**
card_holder_name brand account_no cvv_no expire_date type user ip_address zip_code state telephone name info email	card_holder_name account_no brand cvv_no expiredate status

4.3.6.2 SendAlert Interface

The SendAlert interface will be used share fraud alerts by the different stakeholders as they encounter them. Table 4.18 shows the inputs and outputs of the interface.

Table 4.18: Shows SendAlert Web Service API Parameters

Web Service Name: SendAlert	
Input	**Output**

type user ip_address zip_code state telephone name info email	Success message

4.3.6.3 QueryDetails Interface

The QueryDetails interface will be used fetch detailed information about incidents and alerts collected for a particular card. Table 4.19 shows the inputs and outputs of the interface.

Table 4.19: Shows QueryDetails Web Service API Parameters

Web Service Name: QueryDetails	
Input	**Output**
card_holder_name brand account_no cvv_no expire_date	blacklist details incidents details alerts details

Chapter 5: System Implementation and Testing

5.1 Introduction

The main aim of this research was to implement a collaborative tool that builds up a centralised blacklist of rogue digital financial identities. This dissertation developed a card fraud blacklist prototype to demonstrate the implementation. This chapter goes through how the implementation was done and was tested.

5.2 System Implementation

The prototype implementation comprised of a web based GUI and a restful web service API. The web based GUI is used by to accomplish activities for the individual user. These activities include registration of a user, card registration, linking card to individual user account, reporting incidents and viewing reports. The restful web service API is the integration gateway with all the other card network stakeholders. Services done via the API include; querying of the blacklist database, pushing alerts about reported incidents, pushing alerts about other detected fraudulent digital identity parameters and blacklist of compromised cards. The individual users will access the systems GUI while the API will be accessed by the stakeholder's systems.

The tools used were:

i. Apache webserver to host the web application.
ii. PostgreSQL database connected on port 5432.
iii. NetBeans was used as the development IDE
iv. PHP – PHP was used as server-side scripting language, was used to develop the restful web services to put and fetch records in and from PostgreSQL database.
v. CodeIgniter – provided an MVC (model, view, and controller) framework. Included HTML, CSS and JavaScript.
vi. Postman – is an API development environment used by API developers.

5.3 System Testing

System testing was a vital step of the research conducted, for it enabled the researcher evaluate the functionalities and performance of the developed system based on the user experience, efficiency and effectiveness. The testing process also helped the researcher in identifying system

improvements that could be used in the systems future market versions. Tests done were usability and functionality tests. Usability tests focused on the ease of system use, flawlessness and the understanding of the system. Functionality tests focused on the functional components of the applications.

5.3.1 Functional Testing

The prototype was created to demonstrate that the collaboration of card network association can yield a relevant blacklist database that can assist in reducing financial identity fraud losses. The implementation was done by creating secure channels where each stakeholder can contribute in building up the database, updating the database with their daily encounters and a channel for interrogating the database about a particular identity. The functions that were tested are: whether we can register system users? Can we report incidents of our compromised financial identity cards? Can we create the blacklist database? Can the blacklist database be used? Can we send alerts about any reported financial card? We created test cases of the above questions as a checklist of functional testing. Postman was used as the API input output tool. The test cases are discussed in the subsequent subsections.

5.1.1.1 System Users Registration

The user registration form can be found at Appendix Figure B.1. Below is the test case to validate we can really have users in the system. Figure 5.1 shows the user administration page, this represents the output of user register.

Table 5.1: System User Registration Test Case

Test Case Name: System Users Registration		**Test Case Number 1**	
Brief Description: Application should be able to register system users: Card owners, banks, merchants and the entire card network association.			
Pre-condition: The system is running properly and all its components communicate well.			
Step	**Action**	**Expected results**	**Pass/Fail**

1.	User accesses the register user form by clicking the user sub menu in the register menu.	The registration form opens	Pass
2.	User enters user details and select the stakeholder type appropriately	The user can fill the form and select stakeholder type appropriately	Pass
3.	User saves the user registration details by clicking the save button	User is successfully created and login credentials sent to his mail box	Pass
Post condition: A new user is created in the system.			

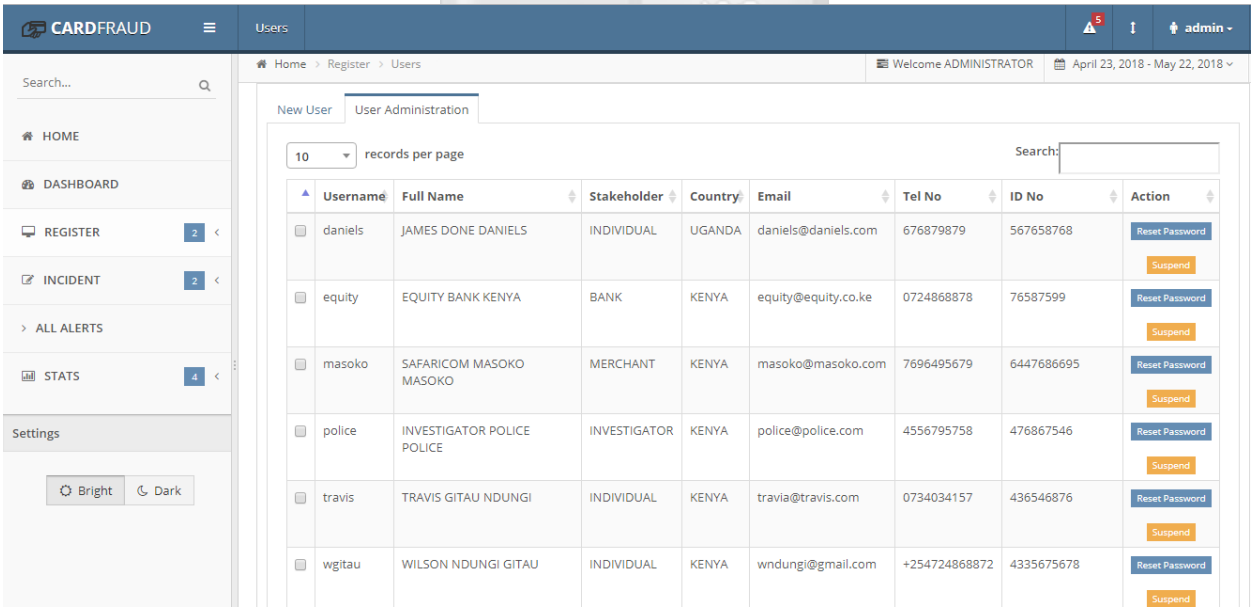


Figure 5.1: Shows Registered System Users

5.1.1.2 System Access

The login form provides access to the system. The login form can be found at Appendix Figure B.2

Table 5.2: System Access Test Case

Test Case Name: System Access		**Test Case Number 2**	
Brief Description: Users should be able to access the system			
Pre-condition: The systems is running properly and all its components communicate well.			
Step	**Action**	**Expected results**	**Pass/Fail**
1.	User accesses the report incident form by clicking the report incident sub menu in the incident menu.	Open login page	Pass
2.	User keys in credentials as shared in the mail box	User is able to key in the credentials	Pass
4.	User clicks the login button	User is redirected to the home page as shown in Appendix Figure B.3	Pass
Post condition: The user has system access			

5.1.1.3 Reporting Incidents

The form used to capture card incident details can be found at Appendix Figure B.4. Below is the test case to validate that we can report an incident about a compromised card. Figure 5.2 shows the output of filing an incident report.

Table 5.3: Reporting Card Incident Test Case

Test Case Name: Reporting Incidents	**Test Case Number 3**
Brief Description: Application should be able to allow reporting of compromised payment cards	
Pre-condition: The systems is running properly and all its components communicate well.	

Step	Action	Expected results	Pass/Fail
1.	User accesses the report incident form by clicking the report incident sub menu in the incident menu.	Incident reporting form opens	Pass
2.	User searches and selects the compromised card that he wants to report	The user can select cards that are on his or her profile	Pass
3.	User fills the incident details in the form	User can populate incident details	Pass
4.	User clicks on save	User saves the incident successfully	Pass
Post condition: An incident is reported and card put on suspend mode in the database			

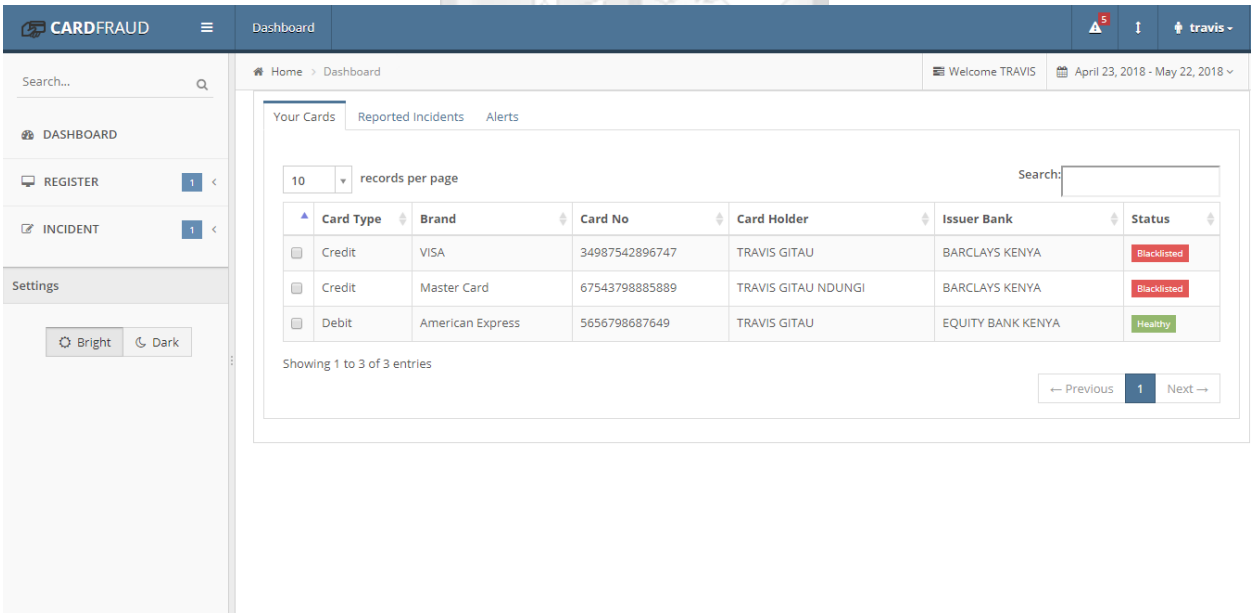


Figure 5.2: Shows Blacklist State of a Card after Incident Report

5.1.1.4 Blacklist Database Query

This is the test of the blacklist database. The objective is to check whether the system blacklists cards reported by incidents, whether it adds other digital financial identity cards in the blacklist, whether it can be queried by a stakeholder and result a correct status of the card or any other digital identity in the financial technology. Appendix Figure B.5 and Appendix Figure B.6 show a query status of a card. Figure B.5 shows a blacklisted query while Figure B.6 show a healthy state card. Appendix Figure C.1 shows Blacklist Database Query API input and Figure 5.3 shows Blacklist Database Query API output. Table 5.4 below shows the backlist query API test cases done using postman.

Table 5.4: Blacklist Database Query Test Case

Test Case Name: Blacklist Database Query		**Test Case Number 4**	
Brief Description: The API should be able query status of the financial digital identity			
Pre-condition: The systems is running properly and all its components communicate well. Have set a HTTP POST request to the server in postman			
Step	**Action**	**Expected results**	**Pass/Fail**
1.	Key in the correct parameters as specified input parameters as specified by QueryBlacklist API input in Appendix Figure C.1	User should be able to key in inputs	Pass
2.	User hits the send request	Receive a response with output parameters as specified by QueryBlacklist API output in Figure 5.3	Pass
Post condition: The system responds with a blacklist status.			

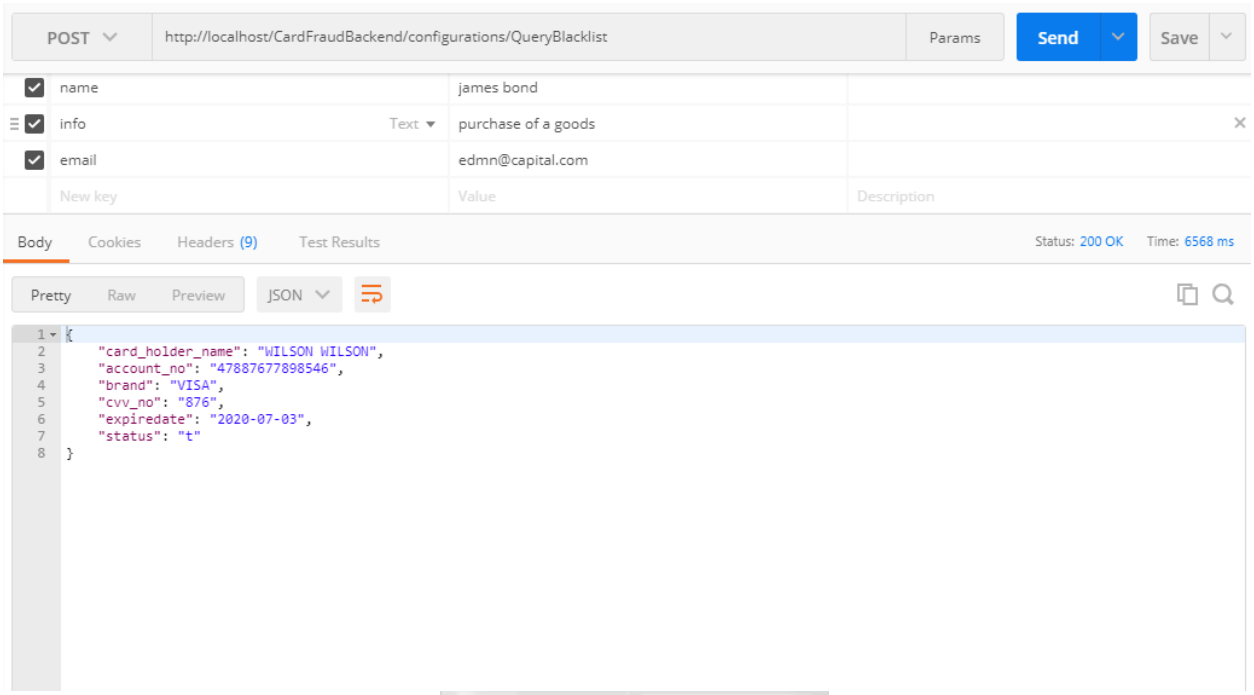


Figure 5.3: Shows the Query Blacklist Web Service Result

5.1.1.5 Send Alerts

The objective of this test case is to check whether the system can accept alerts sent by the stakeholders. Appendix Figure C.2 shows Send Alerts Query API input and Appendix Figure C.3 shows Send Alerts Query API output. Table 5.5 below shows the send alert query API test cases done using postman. Figure 5.4 shows the logged alerts, the output of send alert action.

Table 5.5: Send Alerts Test Case

Test Case Name: Send Alerts			**Test Case Number 5**
Brief Description: The API should be able to accept alerts financial digital identity theft alerts sent by the card network stakeholders.			
Pre-condition: The systems is running properly and all its components communicate well. Have set a HTTP POST request to the server in postman			
Step	**Action**	**Expected results**	**Pass/Fail**

1.	Key in the correct parameters as specified input parameters as specified by SendAlert API input in Appendix Figure C.2	User should be able to key in inputs	Pass
2.	User hits the send request	Receive a response with output parameters as specified by SendAlert API output in Appendix Figure C.3	Pass
Post condition: The system responds to have successfully logged the alerts			

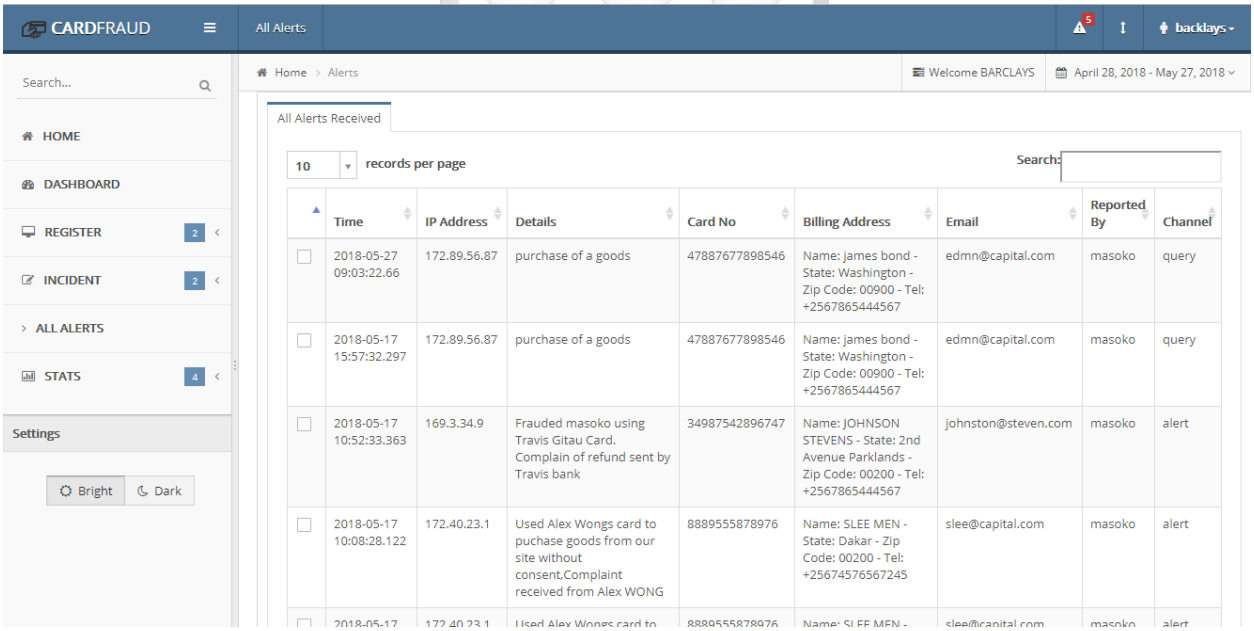


Figure 5.4: Shows the Alerts Logged by the System

5.1.1.6 Querying Detailed Data

The objective of this test case is to check whether we are able to report status, incidents and alerts collected by the system. This information is presented in an API that is consumable by the relevant parties. Appendix Figure C.4 shows Query Details API input and Figure 5.5 shows Query Details API output. Table 5.6 below shows the send alert query API test cases done using postman.

Table 5.6: Query Detailed Data Test Case

Test Case Name: Query Detailed Data			**Test Case Number 6**
Brief Description: The API should be able to query the detailed card report about incidents and logged alerts.			
Pre-condition: The systems is running properly and all its components communicate well. Have set a HTTP POST request to the server in postman			
Step	**Action**	**Expected results**	**Pass/Fail**
1.	Key in the correct parameters as specified input parameters as specified by QueryDetails API input in Appendix Figure C.4	User should be able to key in inputs	Pass
2.	User hits the send request	Receive a response with output parameters as specified by QueryDetails API output in Figure 5.5	Pass
	Post condition: The reports the status, incidents and alerts logged.		

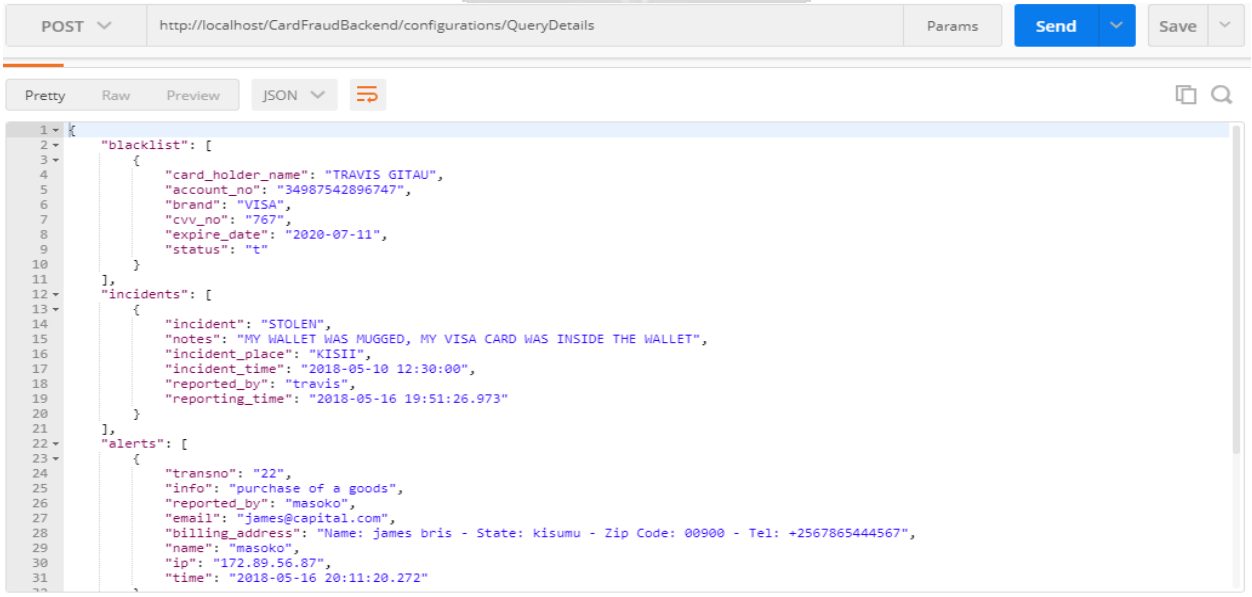


Figure 5.5: Shows the Web Service Result

5.3.2 Usability Testing

Usability testing was carried out to ensure that the system met the aesthetic requirements to enhance the user adopt the system easily. It checks the user friendliness of the system. Table 5.7 Shows the tests carried out to ensure that the usability of the system was satisfactory.

Table 5.7: System Usability Test Cases

Test Case Name: System Usability			**Test Case Number 7**
Brief Description: Test user experience in the application			
Pre-condition: The systems is running properly and all its components communicate well.			
Step	**Action**	**Expected results**	**Pass/Fail**
1.	User can access menus easily	The menus are visible, font is appealing and readable.	Pass
2.	User can select clickable items in the system	Floating icons accessible to users, clickable GUI components can be identified and accessed	Pass

Table 5.8: Web Browser Test Cases

Test Case Name: Web Browser Testing			**Test Case Number 8**
Brief Description: Test done to access system via different web browsers			
Pre-condition: The systems is running properly and all its components communicate well.			
Step	**Action**	**Expected results**	**Pass/Fail**
1.	Internet Explorer – Version 4 and above	Access the system	Pass
2.	Mozilla Firefox – Version 4 and above	Access the system	Pass
3.	Chrome – all versions	Access the system	

5.4 Summary

As part of system testing, it was noted that some of our research objectives and research questions set were achieved. We were able to implement and test an effective system that will help to prevent fraudulent usage of financial cards thus reducing losses incurred by the card industry.

Chapter 6: Discussion of Results

6.1 Introduction

Findings got during this research formed part of the basis on which the proposed card blacklist system was implemented. The implementation was tested to confirm that all the functionalities were working. This chapter analyses the findings in relation to the objectives as stated in Chapter one of this dissertation and the extent to which the findings match with the literature review.

6.2 The Aspects of Digital Identity Theft in Financial Technology

The first objective in section 1.3 was to analyse aspects of digital identity theft in financial technology. From the study findings, it was found that technology uptake has rampantly increased in the financial sector thus driving the use of digital identity, specifically increased ecommerce checkouts using payment cards to complete transactions. The increased use of the digital identities has given rise to digital identity theft. The research in literature review section 2.2 shows that the digital identity fraud crimes have become more common, easier and safer to perform with little risk of getting caught. The literature further shows that in this era identity thieves keep up to date with technology, their driving purpose been the enlarging e-commerce space. Reports cited in the subsection indicate that over the past years card payment fraud has recorded numerous amounts of losses. According to these findings we can conclude that there is dire need to develop schemes that counter this theft.

6.3 Methods Used to Prevent Fraudulent Usage of Financial Cards

The second objective was to review the methods used to prevent fraudulent usage of financial cards. From the study's findings, due to the rampant and gradually increasing card identity theft, methods to detect and identify fraud in credit card are deemed necessary. It shows that the fraudsters are also changing their techniques with time in order to penetrate any new credit card fraud detection system thus creating need for mower schemes to prevent fraud. The literature review discusses the various methods used to prevent credit card fraud and their challenges.

6.4 The Proposed System

The third objective was to develop a system that will reduce and help in investigating fraudulent usage of financial cards. The research findings shows the existing gaps and finds it necessary to have a collaborative card fraud blacklist system in order to reduce card payment fraud. The

researcher developed the blacklist system which creates a centralised blacklist database which is accessible to all stakeholder. Card association stakeholders query the database as a check in transaction processing. This centralised database check reduces the chances of processing a fraudulent card transaction as demonstrated in testing. The system further collect financial cards alerts from the stakeholders which yields rich information which deduce statistical and investigative about a card. This is in line with the objective of our proposed system. The literature review chapter 2.12 discusses the schematic design of the proposed system which is in harmony with the developed system.

6.5 The Proposed System Testing

The last objective was to carry out a test and validate the proposed system. The research methodology chapter discusses two testing approaches which include functional testing and usability testing. The functional testing was to test whether the functional requirements were met as discussed in the literature.

The main functional tests for the solution were to ensure proper collaboration and exchange of information to build up the blacklist database, accept alert which will enrich the database with more information that can be used to deduce informative statistical and investigative data. Tests in chapter five demonstrate successful build of the blacklist database, querying of the blacklist, posting of alerts and clear reporting which is in line with the objective. Usability test cases were also run whose main objective was to quantify the user friendliness of the system. Execution results are shown in Table 6.1.

Table 6.1: Test Functions Results

	Test Function	Execution %	Rating
1.	Enrol stakeholders in the system	100%	✓
2.	Stakeholders ability to send information to blacklist database by reporting an incident	100%	✓
3.	Stakeholders ability to query the blacklist database both in API and GUI interface	100%	✓

4.	Ability to report on incidents and alerts collected	100%	✓
5.	Usability of the system	100%	✓
	Overall execution	100%	✓

Below are the resultant screenshots of the executed tests; Figure 6.1 shows the registered users showing satisfaction of test no 1. Figure 6.2 shows how to report an incident satisfying test no 2. Figure 6.1 and Figure 6.4 shows querying of a card blacklist using GUI and API interface respectively, this satisfies test no 3. Figure 6.2 shows the reporting of incidents and alerts collected by the system satisfying test case no 4. Figure 6.3 shows a granular report of incidents reported by the system, also satisfying test no 4.

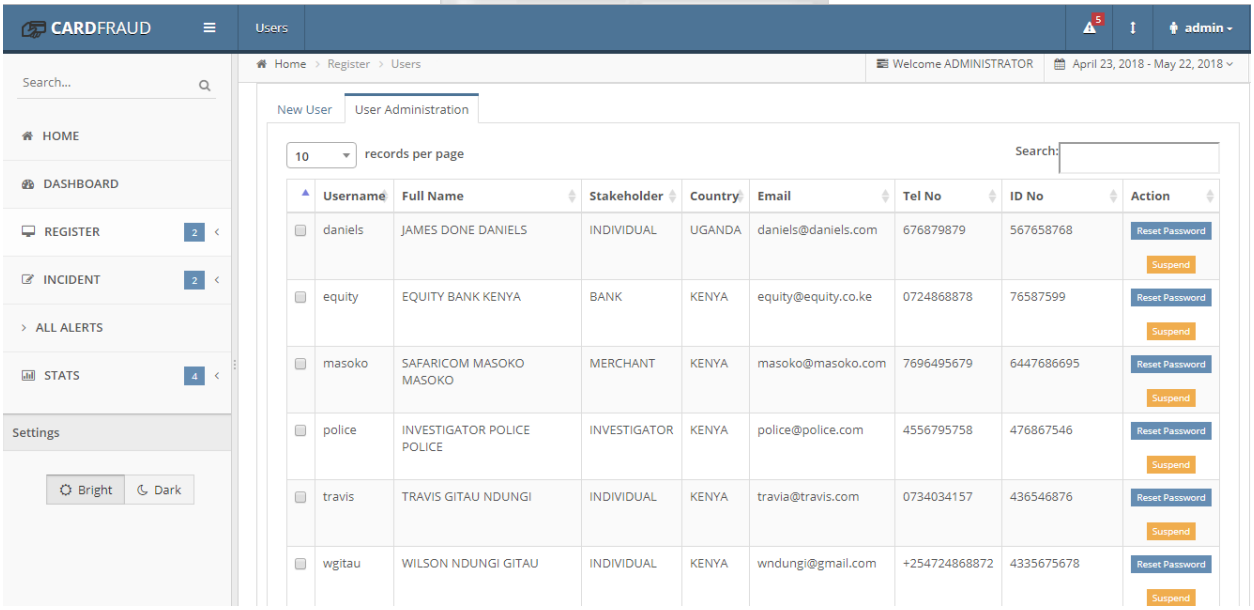


Figure 6.1: Shows the Registered Users

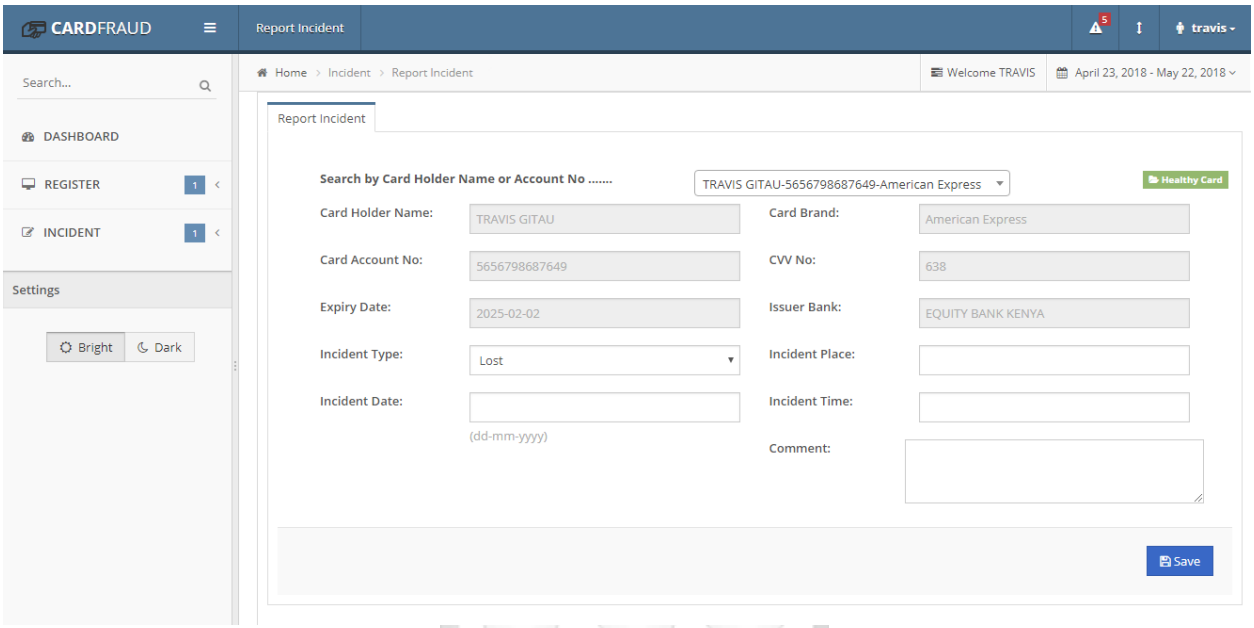


Figure 6.2: Shows how to Report an Incident

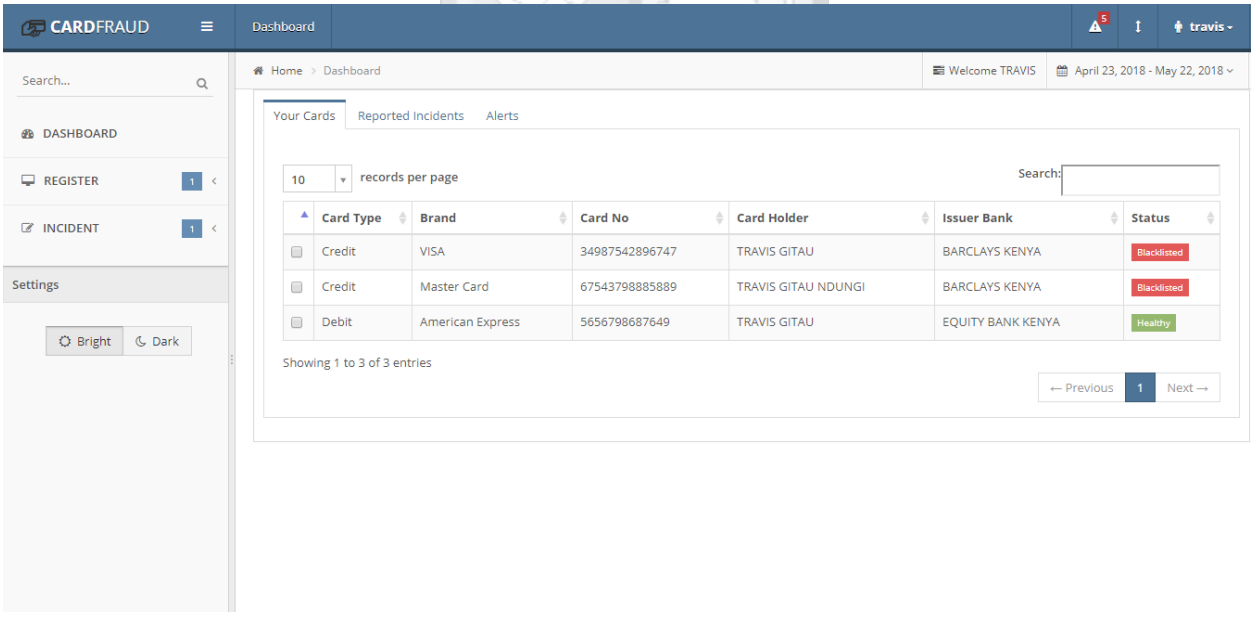


Figure 6.3: Shows Querying of a Card Blacklist Using GUI

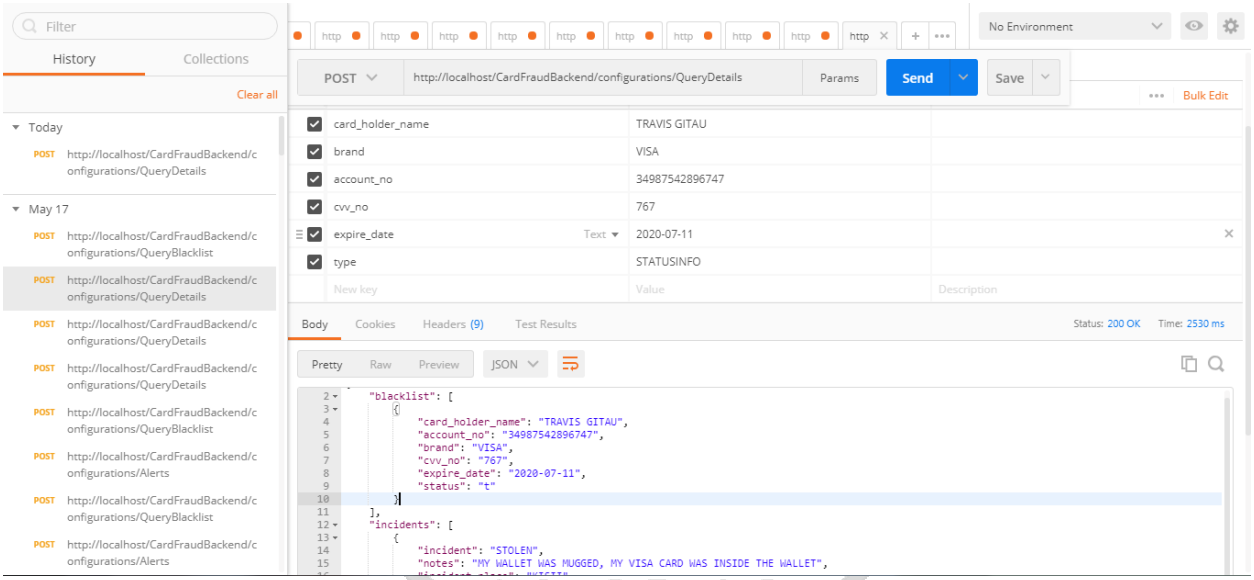


Figure 6.4: Shows Querying of a Card Blacklist Using API Web Service

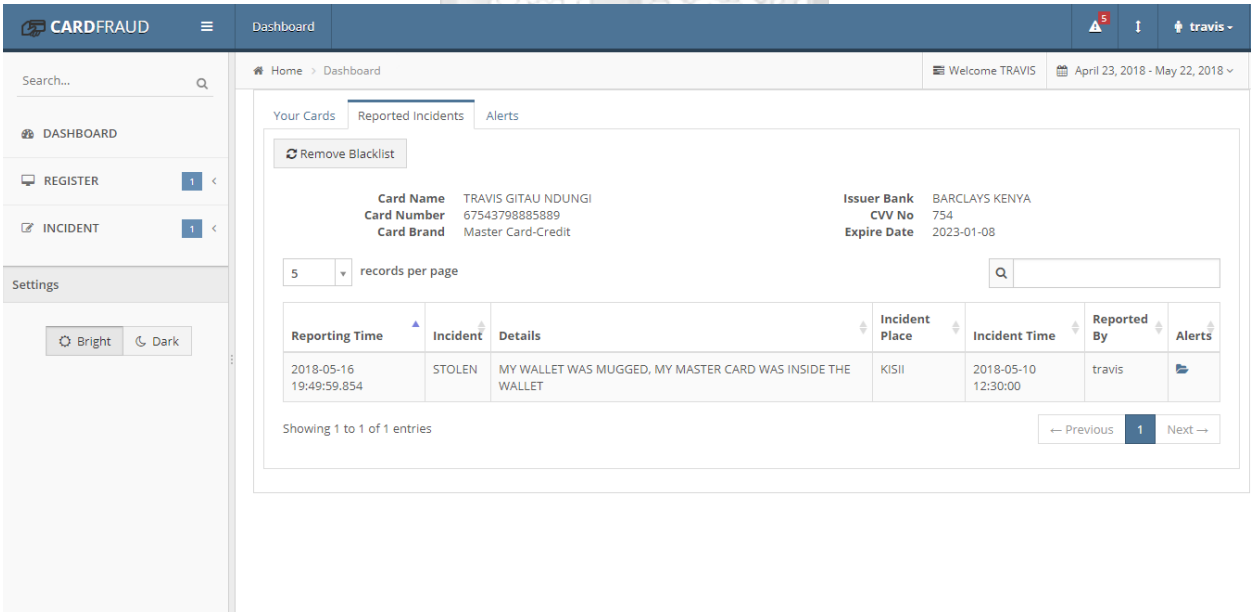


Figure 6.5: Shows the Reporting of Incidents and Alerts

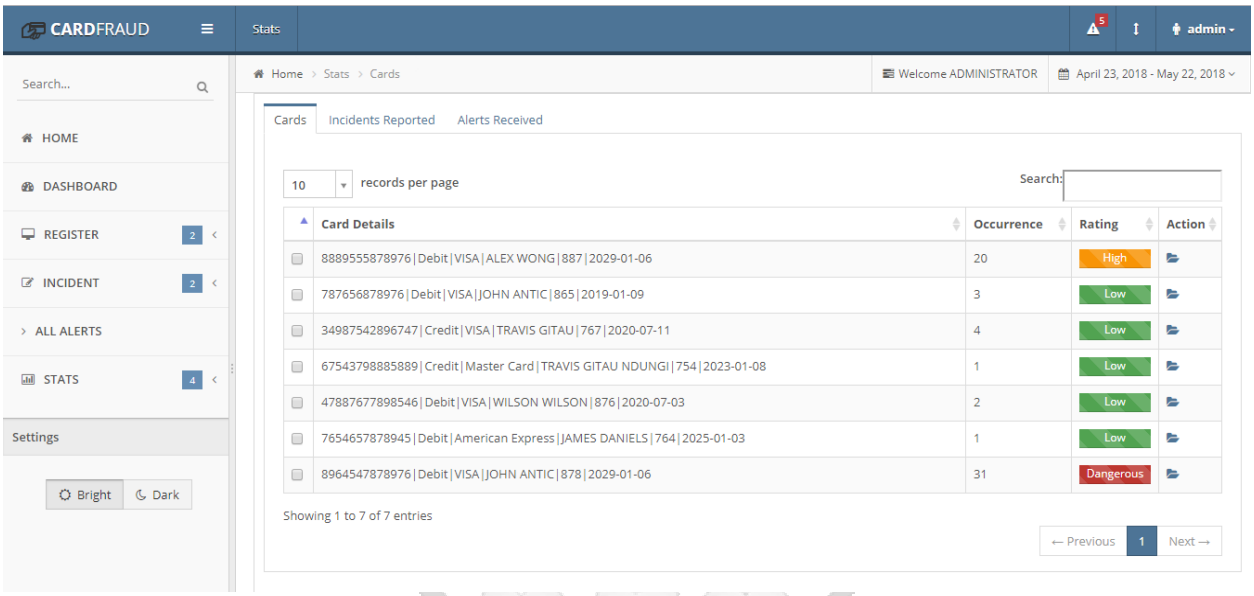


Figure 6.6: Shows a Granular Report of Incidents Reported

6.6 Advantages of the Proposed System

6.6.1 Advantages to Cardholders

They will be able to report incidents about their financial cards immediately without reaching out to the issuer bank as the first level of incident report. This will blacklist his or her card from carrying more transactions, thus reducing the window of manual reporting to the issuer bank.

6.6.2 Advantages to Merchants and Banking

Merchants are the most affected by card fraud, since mostly they are forced to accept full liability of losses when protecting their businesses reputation. A credit card charge dispute by a legitimate card holder leads to a charge back initiated by the issuer bank to the merchant through the acquirer's bank. Having a blacklist checklist will prevent the no of fraudulent cards accepted by merchants thus reducing loses. The chargeback, administrative costs and disputes filed to banks will also reduce.

6.7 Limitations of the Proposed System

The proposed system learning is fully dependent on the collaboration of all the card network association stakeholders. All stakeholders need to share genuine information to the system.

Chapter 7: Conclusions, Recommendations and Future Work

7.1 Introduction

This chapter will look at the conclusion, recommendations and future work that the researcher identified during the research.

7.2 Conclusion

This dissertation analyses aspects of digital identity theft in financial technology. It focuses on payment card fraud, reviewing the methods used to prevent and investigate fraudulent usage of compromised financial cards. It further proposes a system to prevent fraudulent usage of stolen financial digital identity through lost, stolen or compromised payment cards. As the technology advances financial digital identity has risen, thus continuing to record huge amount of losses. Case scenarios of big losses are discussed in the literature. The proposed solution was based on providing a collaborative platform among the card network stakeholders. This platform allows the stakeholders to securely share compromised and fraudulent payment cards and other financial digital identities, thus providing a centralised pool of rogue digital identities called a blacklist. All stakeholders are able to consult the blacklist before finalising a transaction thus ensuring he is not dealing with a rogue digital identity. The research developed the card fraud blacklist prototype to demonstrate a collaboration that reduces financial digital identity fraud. The proposed card fraud system was tested using sample data, demonstrating various scenarios and activities of financial card usage. The collaborative nature of the system ensured when one stakeholder learns of a fraudulent financial digital identity all the other stakeholders are aware of the rogue identity, thus lesser surface of fraud. APIs to all stakeholders were tested and resulted to a simple collaborative tool to reduce losses made by digital financial identity theft.

7.3 Recommendation

The proposed system demonstrated a collaborative way to reduce financial digital identity theft fraud using information technology. Financial digital identity theft especially in card payment process has recorded huge losses as reviewed in the literature. The literature further show that all the stakeholders; card owners, merchants and banks (acquirers and issuers) are largely impacted by this kind of theft. The research recommends all the stakeholders to integrate with this

collaborative tool so as to eliminate unnecessary losses from digital identity theft in financial technology.

7.4 Future Work

The researcher intends to develop a market version of the system. Due to numerous number of financial transactions we will fully implement PCI Standards and incorporate usage of more scalable tools such as NoSQL databases to provide superior performance.

References

Akers, D., Golter, J., Lamm, B., & Solt, M. (2005). Overview of Recent Developments in the Credit Card Industry. *FDIC BANKING REVIEW*, VOLUME 17, NO. 3.

Aliyu, A. A., & Tasmin, R. B. (2012). The Impact of Information and Communication on Banks Performance and Customer Service Delivery in the Banking. *Int. J Latest Trends Fin. Eco. Sc*, Vol-2 No. 1.

Bahnsen, A. C., Aouada, D., & Stojanovic, A. (2015). Detecting Credit Card Fraud Using Periodic Features. *IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 208 - 213.

Balasubramanian, & R Sivakumar, N. (2015). Fraud Detection in Credit Card Transactions:Classification, Risks and Prevention Techniques. *International Journal of Computer Science and Information Technologies*, Vol. 6 (2) , 2015, 1379-1386.

Bhattacharya, M., & West, J. (2016). An investigation on experimental issues in financial fraud mining. *IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, 1796 - 1801.

Chilisa, B. (2012). *Indigenous Research Methodologies.* SAGE.

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime, Vol. 22 Issue: 4*, 492-512.

Dara, J., & Gundemoni, L. (2006). *Credit Card Security and E-Payment.* Lulea University of Technology.

European Payment Council. (2017). *2017 PAYMENT THREATS AND FRAUD.* EPC214-17v1.0.

Githui, D. M. (2011). Mobile Money Transfer in Kenya: An Ethical Perspective. *Research Journal of Finance and Accounting*.

GreenPath, I. (2018, 2 9). *Types of Credit Cards*. Retrieved from GreenPath Financial Wellness: http://www.greenpath.com/resources-tools/financial-education/credit-cards/types-credit-cards

Hayashi, F., Markiewicz, Z., & Sullivan, R. J. (2016). Chargebacks: Another Payment Card Acceptance Cost for Merchants. *Federal Reserve Bank of Kansas City*.

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds,techniques and prevention. *Journal of Law and Conflict Resolution Vol. 4(1)*, 1-12.

Hunt , R. M. (2003). AN INTRODUCTION TO THE ECONOMICS OF PAYMENT CARD NETWORKS. *Federal Reserve Bank of Philadelphia* .

Ignacio, M., & Radcliffe, D. (2011). Mobile Payments Go Viral M-PESA in Kenya. *http://siteresources.worldbank.org*, 353-369.

Immobilise.com. (2018). The National Property Register, for Phones, Gadgets, Bicycles & More.... [online] Available at: https://www.immobilise.com/ [Accessed 25 May 2018].

Joyner, E. (2011). Enterprisewide Fraud Management. *Banking, Financial Services and Insurance* (p. 029). USA: SAS Global Forum.

Justice.gov. (2017, 11 19). Retrieved from Identity Theft | CRIMINAL-FRAUD | Department of Justice: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Kong, S. (2007). *Agile Software Development Methodology: Effects on Perceived Software and the cultural context for organizational adoption.* ProQuest.

Kosemani, T. H., Aghili, S., & Zavar, P. (2016). The use of predictive analytics technology to detect credit card fraud in Canada. *11th Iberian Conference on Information Systems and Technologies (CISTI) - IEEE*, 1-6.

Levitin, A. J. (2011). PAYMENT CARD FRAUD LIABILITY RULES . *Journal of Law*.

Malini, N., & Pushpa, M. (2017). Analysis on credit card fraud identification techniques based on KNN and outlier detection. *2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 255 - 258.

Mandal, P. (2014). Proceedings of the International Conference on Managing the Asian Century. *Business & Economics* (p. 249). Springer Science & Business Media.

Meredith, L. (2017, 11 19). *SIM card crime ring arrested, is your phone safe?* Retrieved from msnbc.com: http://www.nbcnews.com/id/39403547/ns/technology_and_science-tech_and_gadgets/t/sim-card-crime-ring-arrested-your-phone-safe/#.WhHTvFWWbIV

Miller, J. (2007). *Making the Most of the Internet.* Lulu.com.

Nakhumwa, J. N. (2013). Adoption of E-commerce Payment Systems by Commercial Banks in Kenya. *University of Nairobi*.

Ngai, E., Hu, Y., & Yijun, C. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Elsevier B.V.*, Pages 559-569, Volume 50, Issue 3.

(2016). *Nilson Report.* Washington DC: David Robertson.

Ogwueleka , F. N. (2011). DATA MINING APPLICATION IN CREDIT CARD FRAUD DETECTION SYSTEM. *Journal of Engineering Science and Technology,* Vol. 6, No. 3 (2011) 311 - 322 .

Papaa, F., & Jamei, S. M. (2015). Smart Fraud Detection Systems for Credit Cards: Challenges and Solutions. *International Academic Journal of Innovative Research*, Vol. 2, No. 12, pp. 37-43.

Parsons, D. (2012). *Refining Current Practices in Mobile and Blended Learning: New Applications ...* New Zealand: IGI Global.

Paul, B. T., Prabhu, V., & Dua, A. (2003). Understanding Credit Card Frauds. *citeseer*. Retrieved from Tata Consultancy Services.

PCI. (2018, 01 12). *Understanding the Payment Card Industry Data Security Standard version 2.0*. Retrieved from Pcisecuritystandards.org: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Prabowo, H. Y. (2010). Trends in Credit Card Fraud Prevention in the United States, the United Kingdom, Australia and Indonesia. *Centre for Transnational Crime Prevention, University of Wollongong*.

Randhawa, K., Loo, C. K., & Seera, M. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access*, 1-1.

Sadeghi, A.-R. (2013). *Financial Cryptography and Data Security.* Springer.

(2017). *Safaricom Annual Report.* Nairobi: Safaricom.

Sakharova, I. (2012). Payment card fraud: Challenges and solutions. *Intelligence and Security Informatics (ISI), IEEE International Conference*.

Samsung. (2017). *Samsung*. Retrieved from FInd my mobile: http://www.samsung.com/global/galaxy/apps/find-my-mobile/

SAP. (2016). *SAP Annual Report.* Washington, D.C. 20549: SAP SE.

Shiv, K., Ayushi, A., & Mishra, A. K. (2015). Credit Card Fraud Detection: A case study. *Computing for Sustainable Global Development (INDIACom), 2nd International Conference, IEEE*.

Smart Insights. (2017, 11 19). Retrieved from Online Retail growth statistics | Smart Insights: https://www.smartinsights.com/tag/online-retail-growth-statistics/

Spann, D. D. (2014). *Fraud Analytics: Strategies and Methods for Detection and Prevention.* Wiley.

Spencer, T. (2013). *Personal Security: A Guide for International Travelers.* CRC.

Police.ucdavis.edu. (2018). Lost and Found | UC Davis Police Department | Dedicated to collaboration and partnership with the campus community. [online] Available at: http://police.ucdavis.edu/lost-and-found/index.html [Accessed 25 May 2018].

Tripathi, K. K., & Pavaskar, M. A. (2012). Survey on Credit Card Fraud Detection Methods. *International Journal of Emerging Technology and Advanced Engineering*, 2(11).

(2016). *Visa Annual Report.* USA: Visa.

Ucpd.berkeley.edu. (2018). Lost and Found | Police Department (UCPD). [online] Available at: https://ucpd.berkeley.edu/services/lost-and-found [Accessed 25 May 2018].

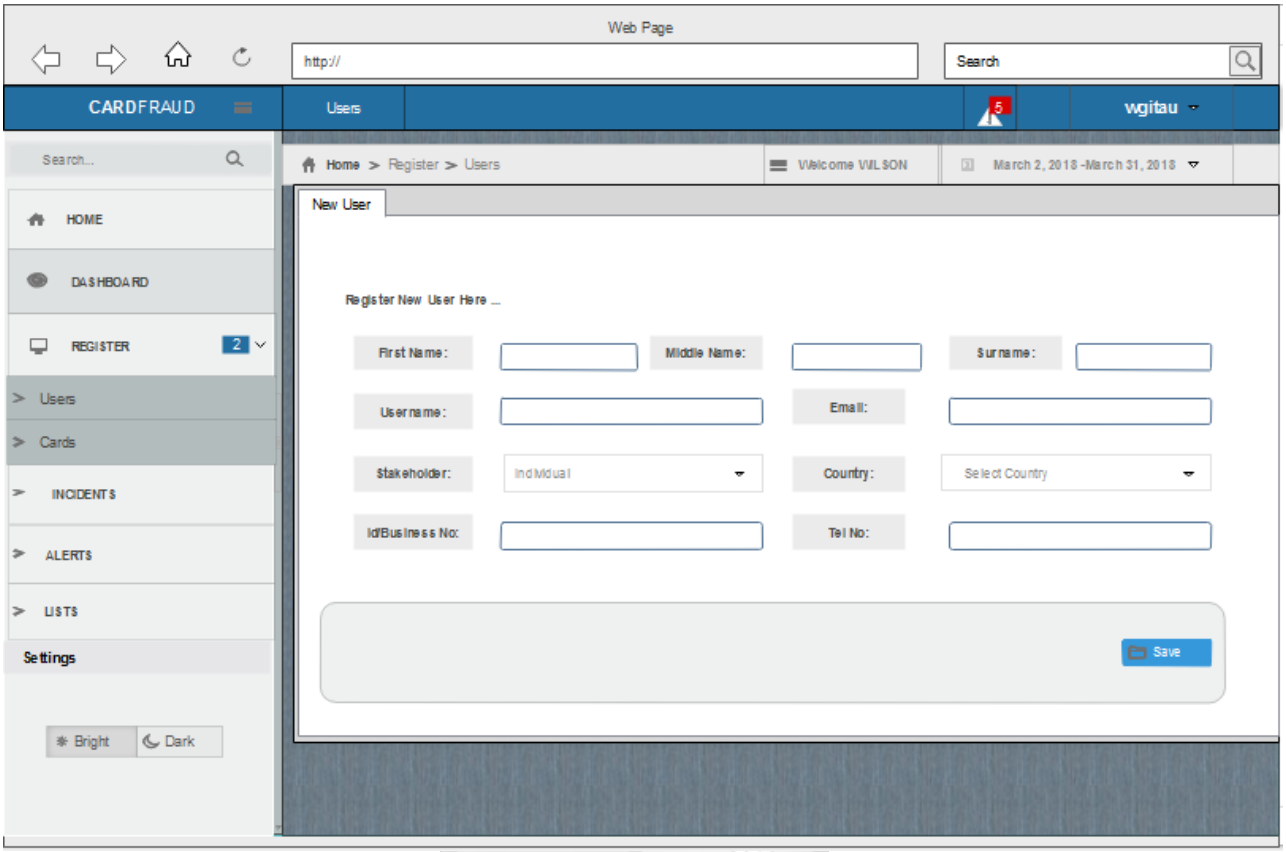
West, J., & Bhattacharya, M. (2015). Some Experimental Issues in Financial Fraud Detection: An Investigation. *IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 1155 - 1158.

Xhafa, F. (2013). An efficient PHR service system supporting fuzzy keyword search and fine-grained access control. *Soft Computing*, 1795-1802.

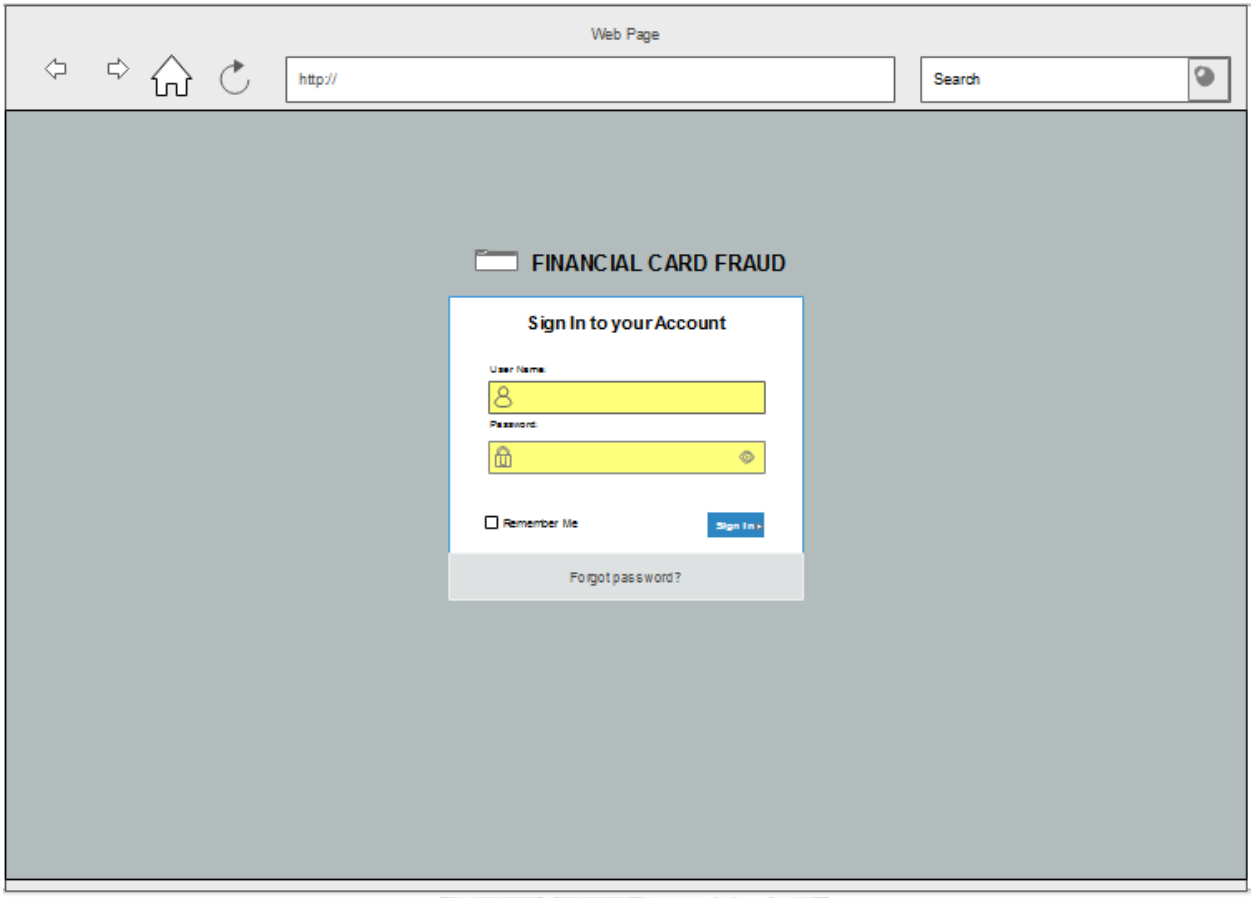
Zareapoora, M., & Shamsolmoal, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. *International Conference on Intelligent Computing, Communication and Convergence*, 679-685.

Appendices

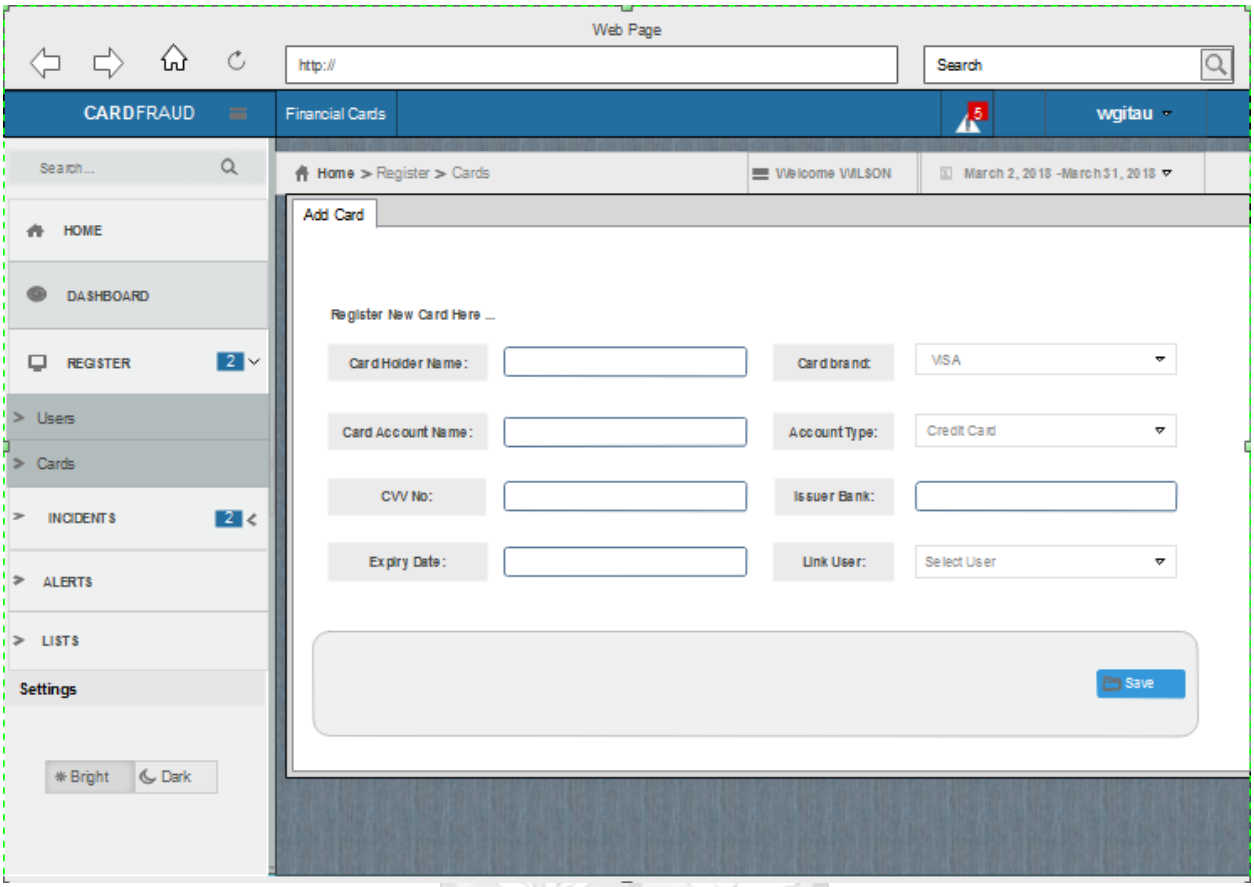
Appendix A: Wireframes



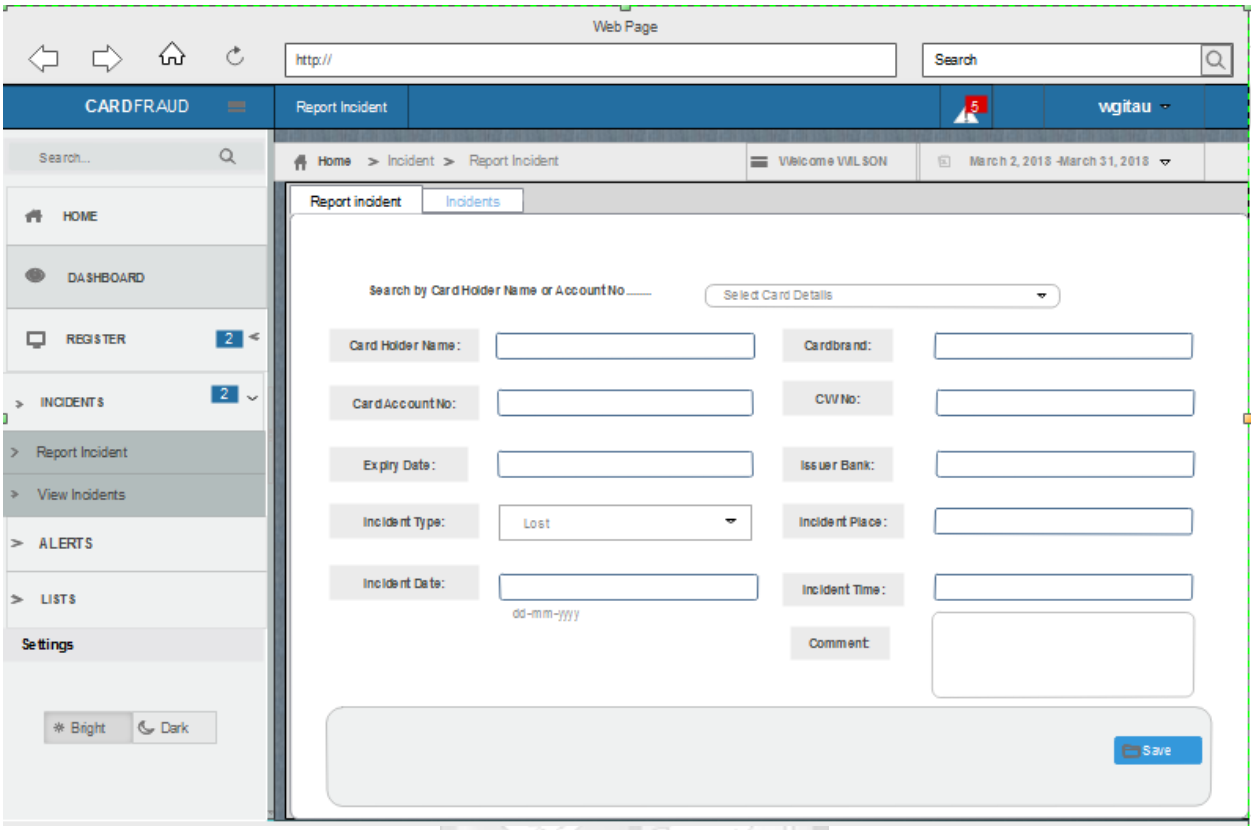
Appendix Figure A.1: Wireframe for User Registration



Appendix Figure A.2: Wireframe for Login Page

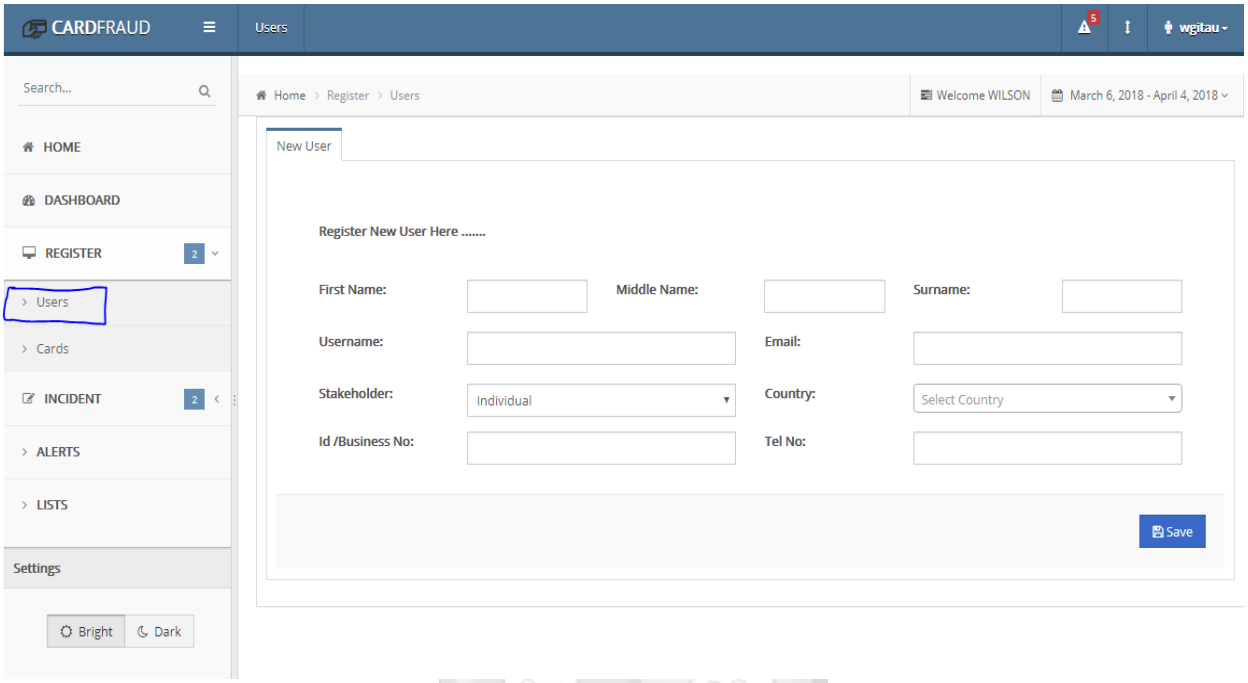


Appendix Figure A.3: Wireframe for Card Registration

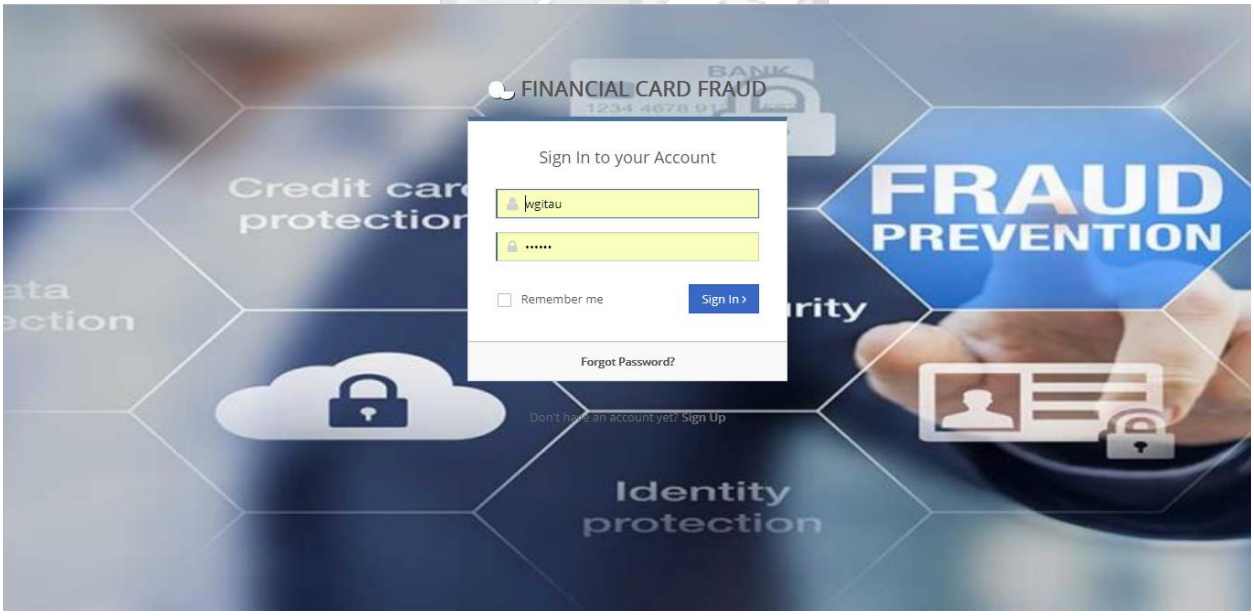


Appendix Figure A.4: Wireframe for Reporting Incidents

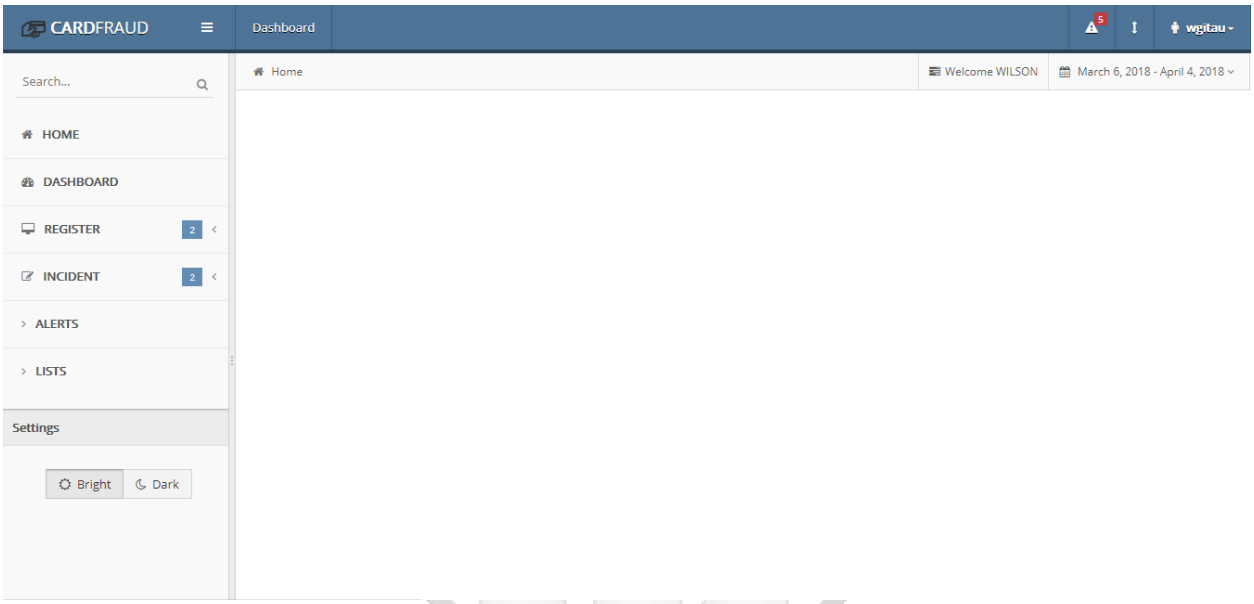
Appendix B: Screenshots



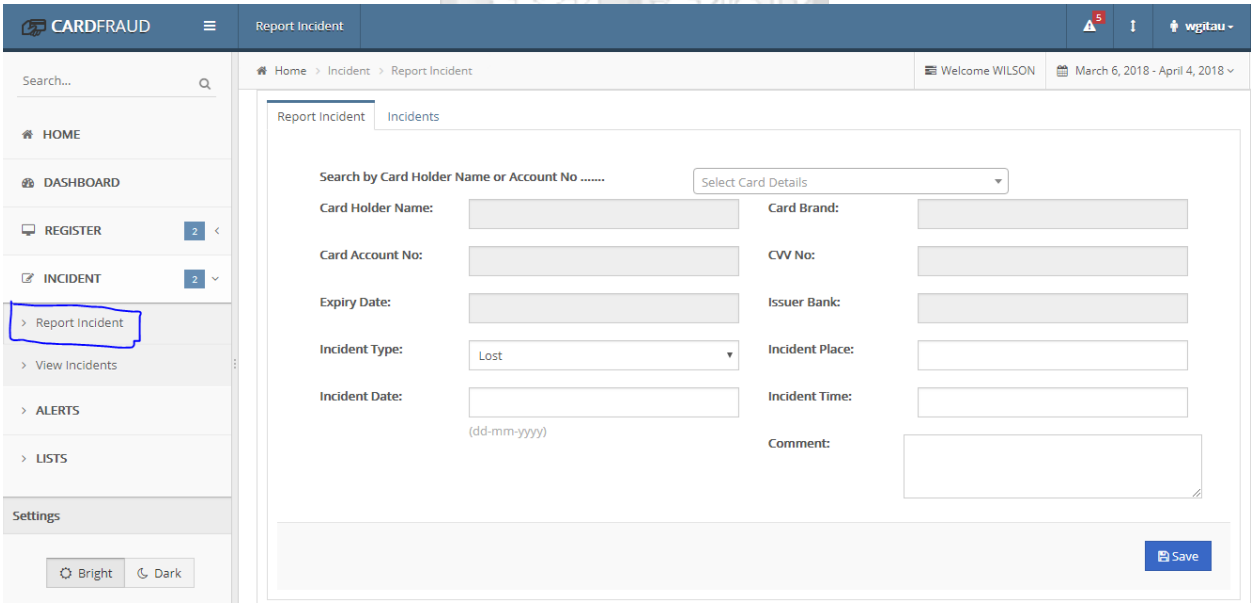
Appendix Figure B.1: Shows the User Registration Form



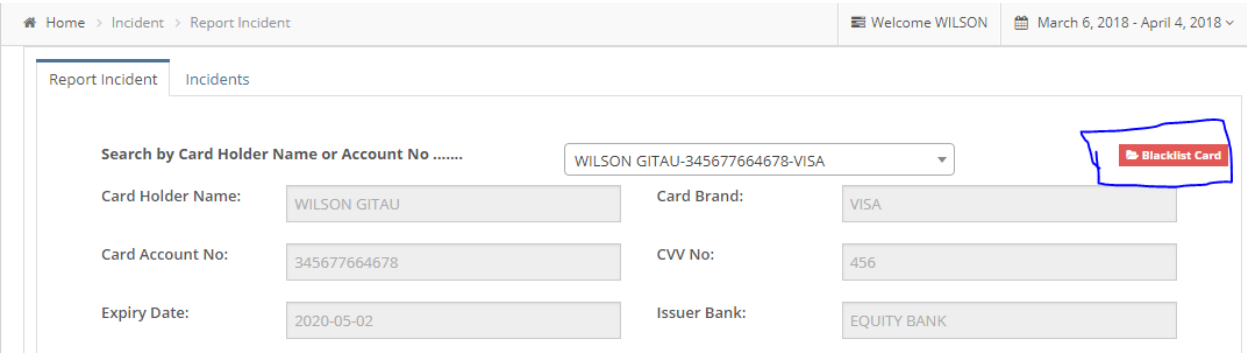
Appendix Figure B.2: Shows the Login Form



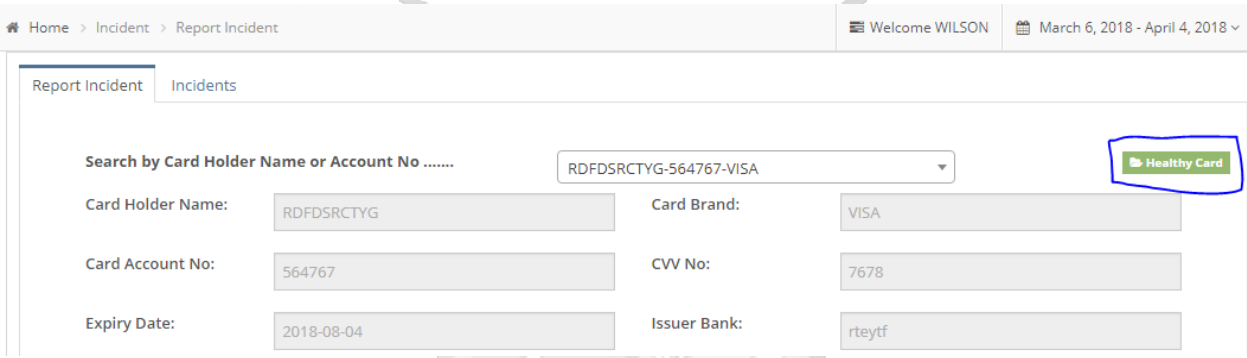
Appendix Figure B.3: Shows the System Home Page



Appendix Figure B.4: Shows the Incident Reporting Form

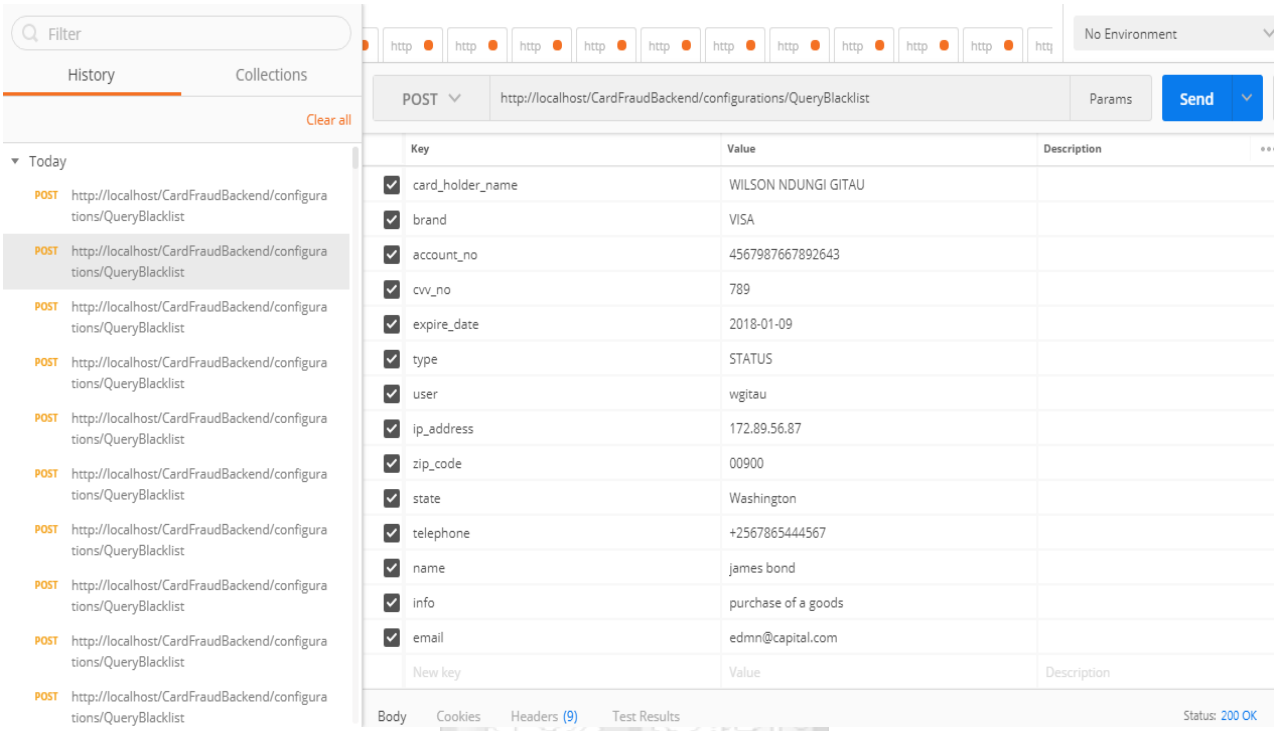


Appendix Figure B.5: Shows Query of a Blacklist Card

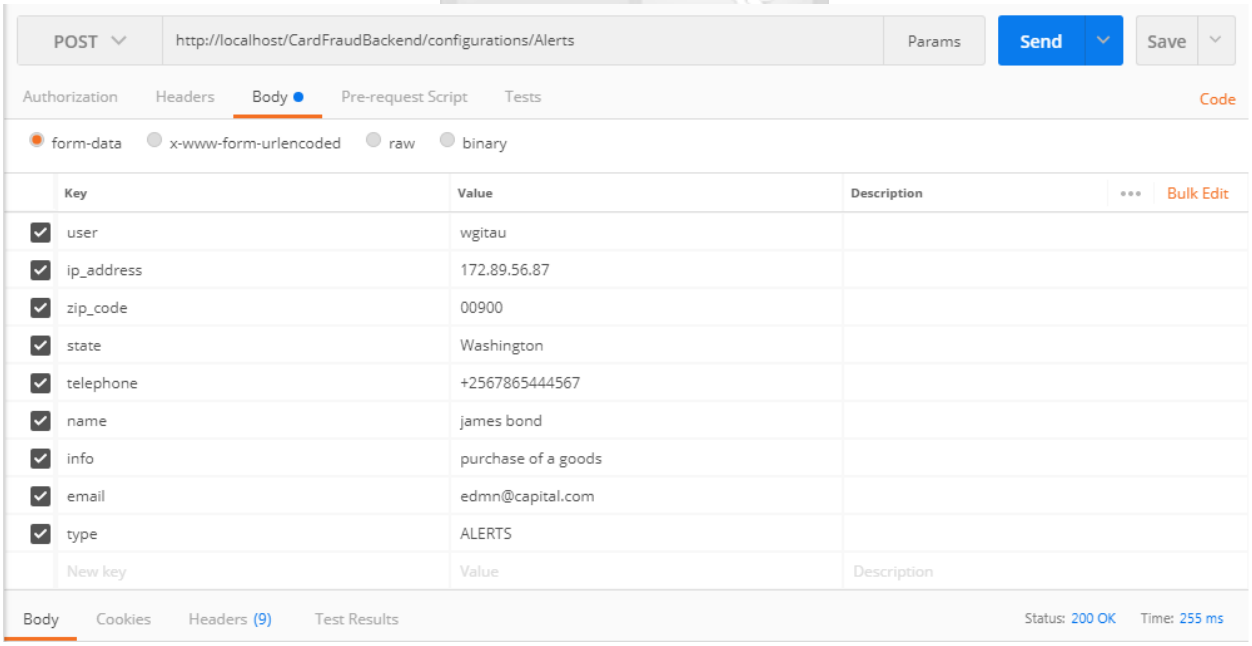


Appendix Figure B.6: Shows Query of a Healthy Card

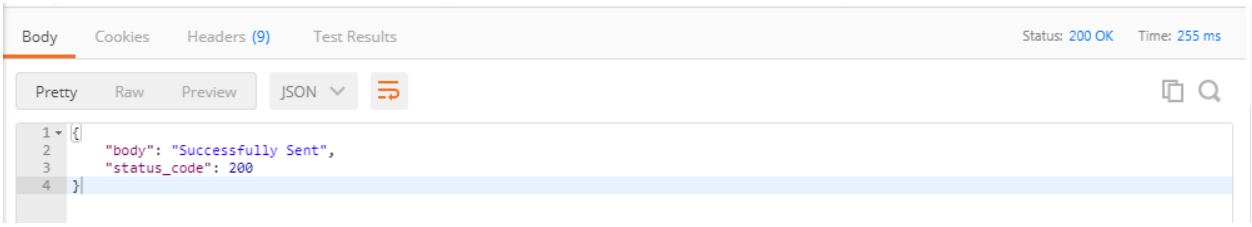
Appendix C: Application Interfaces



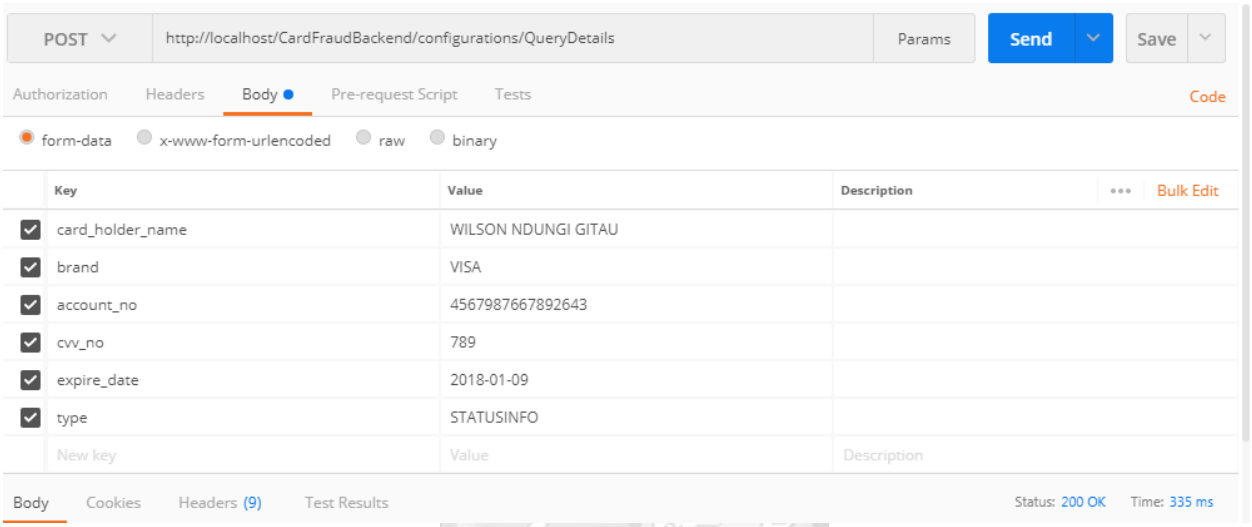
Appendix Figure C.1: Shows the Inputs of QueryBlacklist API



Appendix Figure C.2: Shows the Input parameters for SendAlert Webservice

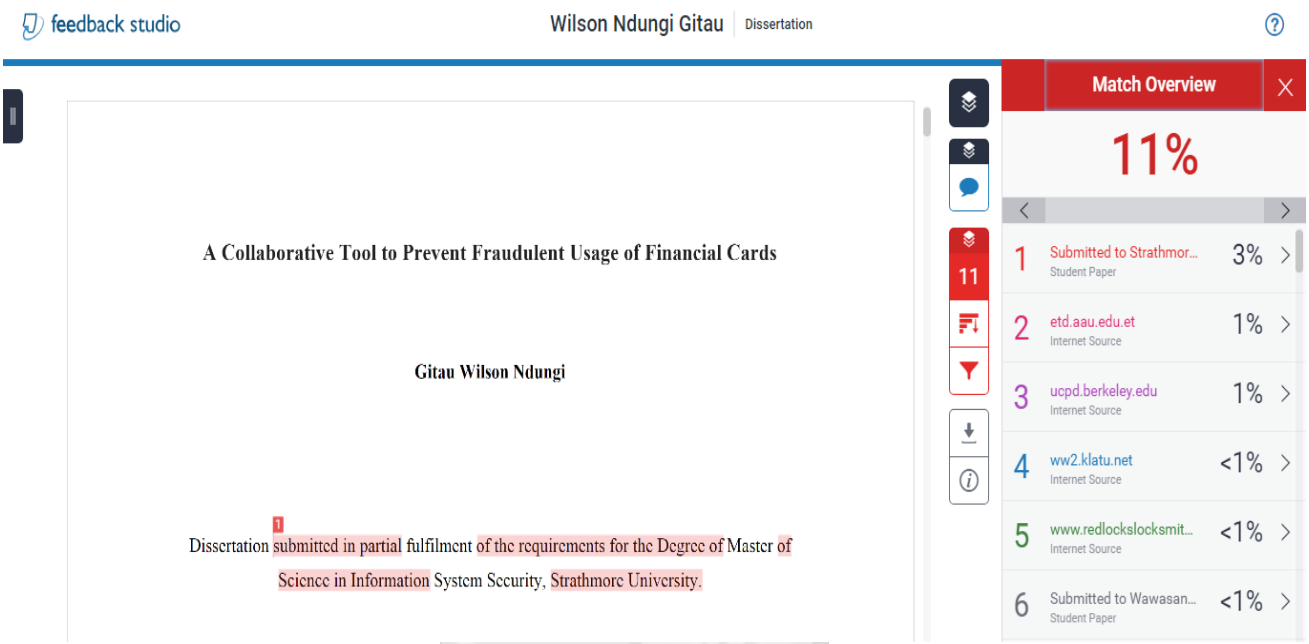


Appendix Figure C.3: Shows the Output for SendAlert Web service



Appendix Figure C.4: Shows the Input Parameters for QueryDetails Web service

Appendix D: Turn it-in Report



Appendix Figure D.1: Turnitin Report