



Strathmore
UNIVERSITY

Strathmore University
SU+ @ Strathmore
University Library

Electronic Theses and Dissertations

2018

A Collaborative tool to prevent fraudulent usage of financial cards

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

Follow this and additional works at <https://su-plus.strathmore.edu/handle/11071/5987>

Recommended Citation

Gitau, W. N. (2018). *A Collaborative tool to prevent fraudulent usage of financial cards* (Thesis).
Strathmore University. Retrieved from <https://su-plus.strathmore.edu/handle/11071/5987>

This Thesis - Open Access is brought to you for free and open access by DSpace @Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @Strathmore University. For more information, please contact librarian@strathmore.edu

Table of Contents

Declaration and Approval	ii
Abstract	iii
Acknowledgements	iv
List of Figures	viii
List of Tables	x
Abbreviations/ Acronyms	xi
Chapter 1: Introduction	1
1.1 Background of Study	1
1.2 Problem Statement	3
1.3 Research Objectives	3
1.4 Research Questions	4
1.5 Scope and Limitation	4
1.6 Justification	4
Chapter 2: Literature Review	5
2.1 Introduction	5
2.2 Digital Identity Fraud	5
2.3 Financial Cards	6
2.4 Financial Cards Network Structure	6
2.5 Financial Card Payment Transaction Flow	7
2.6 Overview of Financial Card Fraud	8
2.7 Techniques Used in Card Fraud	9
2.7.1 Card Related Fraud	9
2.7.2 Merchant Related Fraud	10
2.7.3 Internet Related Fraud	11
2.8 Impact Caused by Financial Card Fraud	11
2.8.1 Impact on Cardholders	11
2.8.2 Impact on Merchants	12
2.8.3 Impact on Banks (Issuers and Acquirers)	12
2.9 Techniques Used to Prevent and Manage Financial Card Fraud	12

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.

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.			

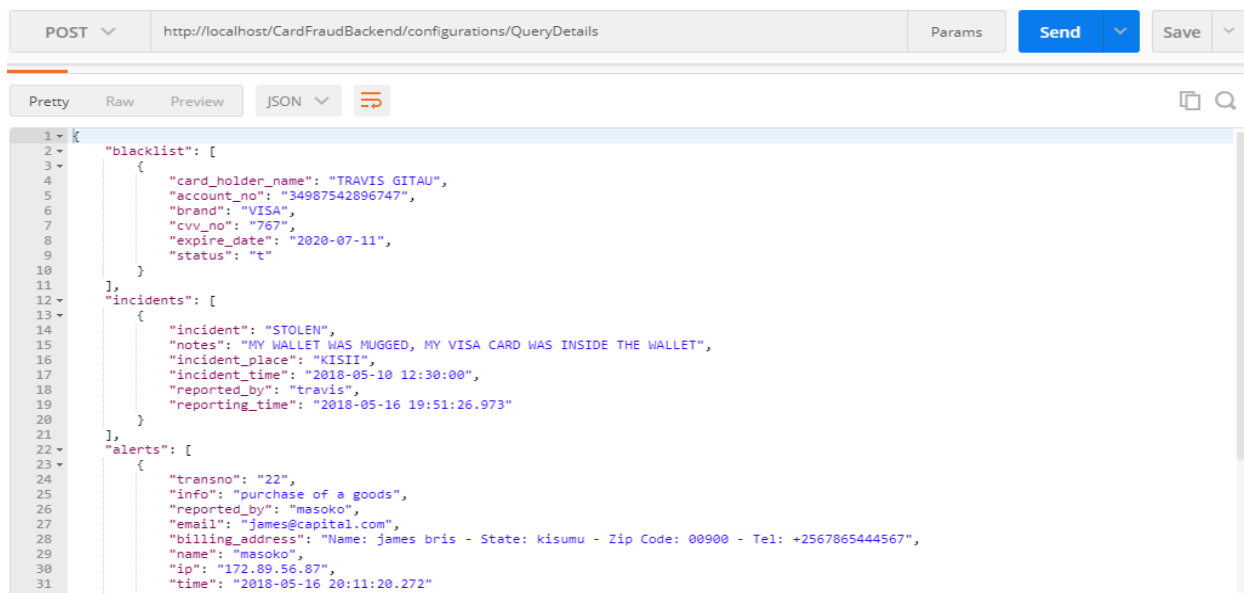


Figure 5.5: Shows the Web Service Result

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.

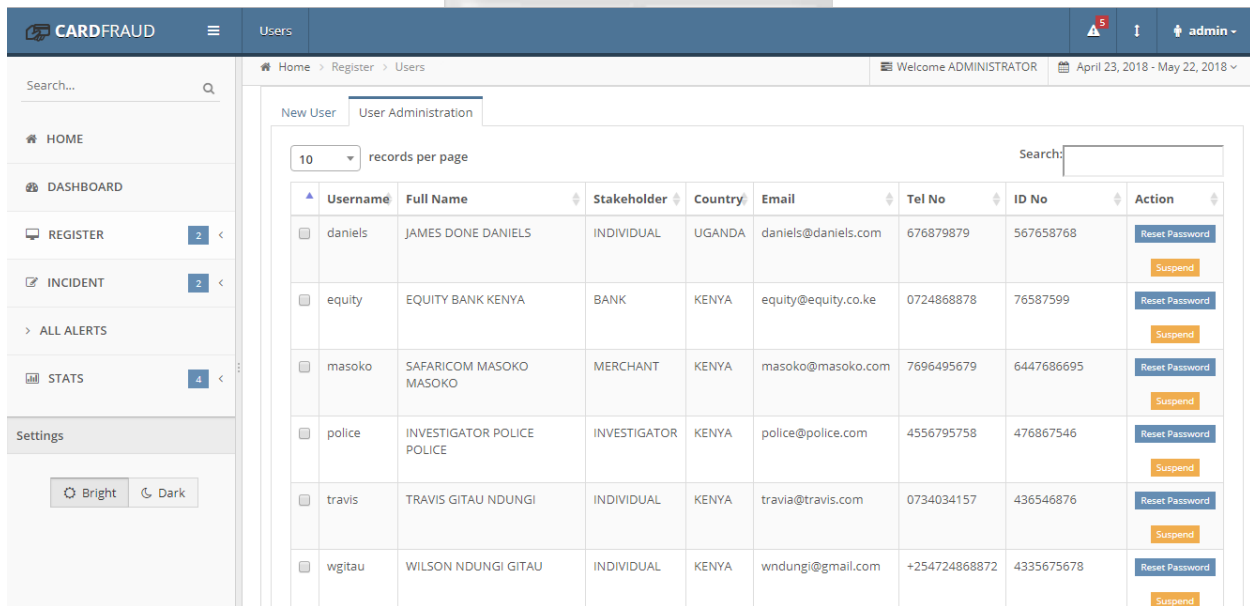


Figure 6.1: Shows the Registered Users

Report Incident

Search by Card Holder Name or Account No TRAVIS GITAU-5656798687649-American Express Healthy Card

Card Holder Name: TRAVIS GITAU Card Brand: American Express

Card Account No: 5656798687649 CVV No: 638

Expiry Date: 2025-02-02 Issuer Bank: EQUITY BANK KENYA

Incident Type: Lost Incident Place:

Incident Date: (dd-mm-yyyy) Incident Time:

Comment:

Save

Figure 6.2: Shows how to Report an Incident

Dashboard

Your Cards | Reported Incidents | Alerts

10 records per page Search:

Card Type	Brand	Card No	Card Holder	Issuer Bank	Status
<input type="checkbox"/> Credit	VISA	34987542896747	TRAVIS GITAU	BARCLAYS KENYA	Blacklisted
<input type="checkbox"/> Credit	Master Card	67543798885889	TRAVIS GITAU NDUNGI	BARCLAYS KENYA	Blacklisted
<input type="checkbox"/> Debit	American Express	5656798687649	TRAVIS GITAU	EQUITY BANK KENYA	Healthy

Showing 1 to 3 of 3 entries

← Previous 1 Next →

Figure 6.3: Shows Querying of a Card Blacklist Using GUI

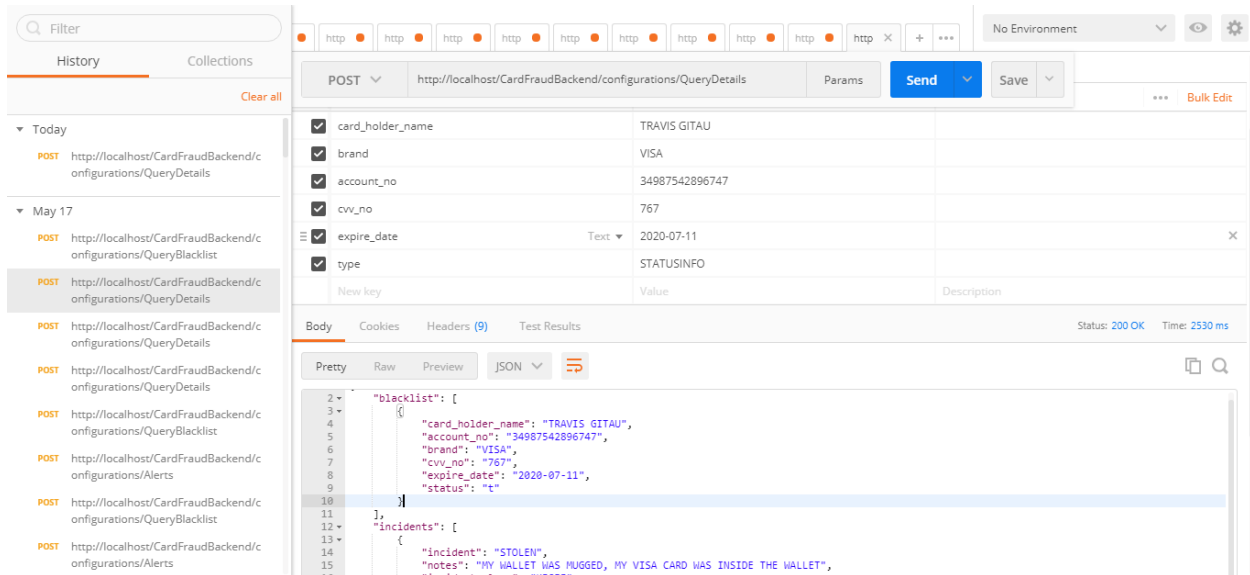


Figure 6.4: Shows Querying of a Card Blacklist Using API Web Service

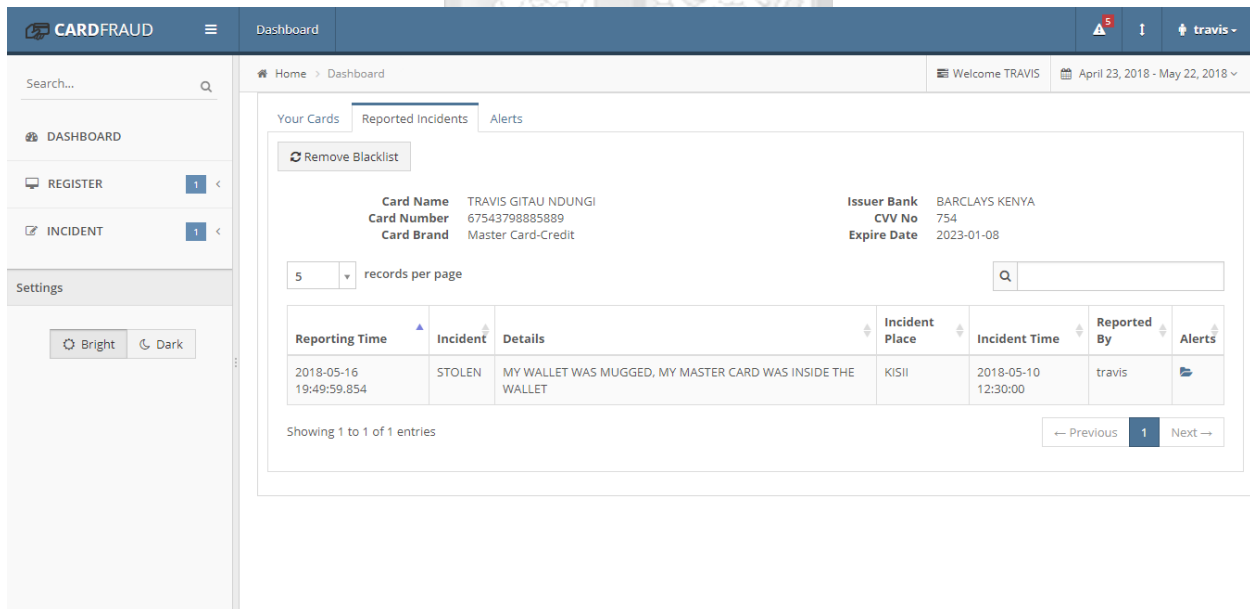


Figure 6.5: Shows the Reporting of Incidents and Alerts

Card Details	Occurrence	Rating	Action
8889555878976 Debit VISA ALEX WONG 887 2029-01-06	20	High	
787656878976 Debit VISA JOHN ANTIC 865 2019-01-09	3	Low	
34987542896747 Credit VISA TRAVIS GITAU 767 2020-07-11	4	Low	
67543798885889 Credit Master Card TRAVIS GITAU NDUNGI 754 2023-01-08	1	Low	
47887677898546 Debit VISA WILSON WILSON 876 2020-07-03	2	Low	
7654657878945 Debit American Express JAMES DANIELS 764 2025-01-03	1	Low	
8964547878976 Debit VISA JOHN ANTIC 878 2029-01-06	31	Dangerous	

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](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*.

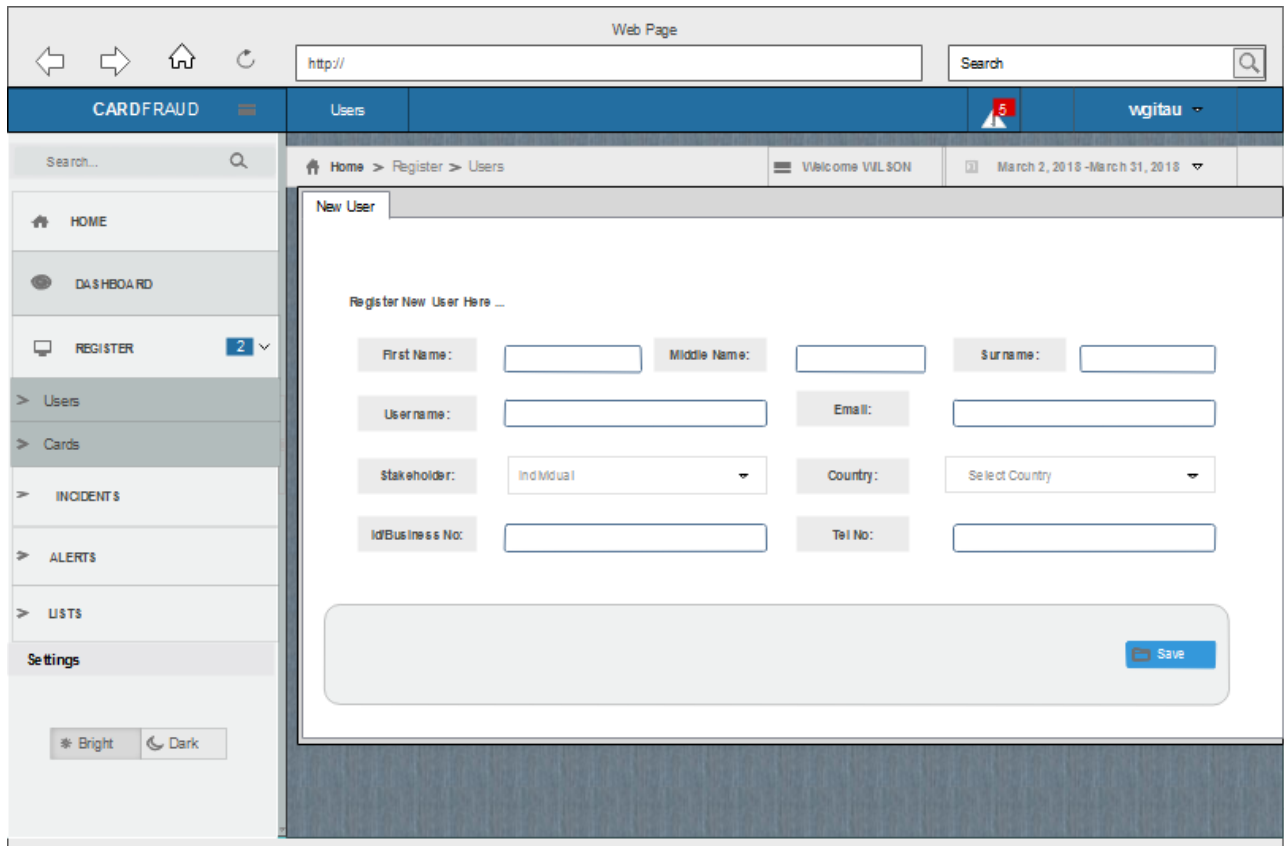
Samsung. (2017). *Samsung*. Retrieved from [Find my mobile: http://www.samsung.com/global/galaxy/apps/find-my-mobile/](http://www.samsung.com/global/galaxy/apps/find-my-mobile/)

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.
- Zareapoor, 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.

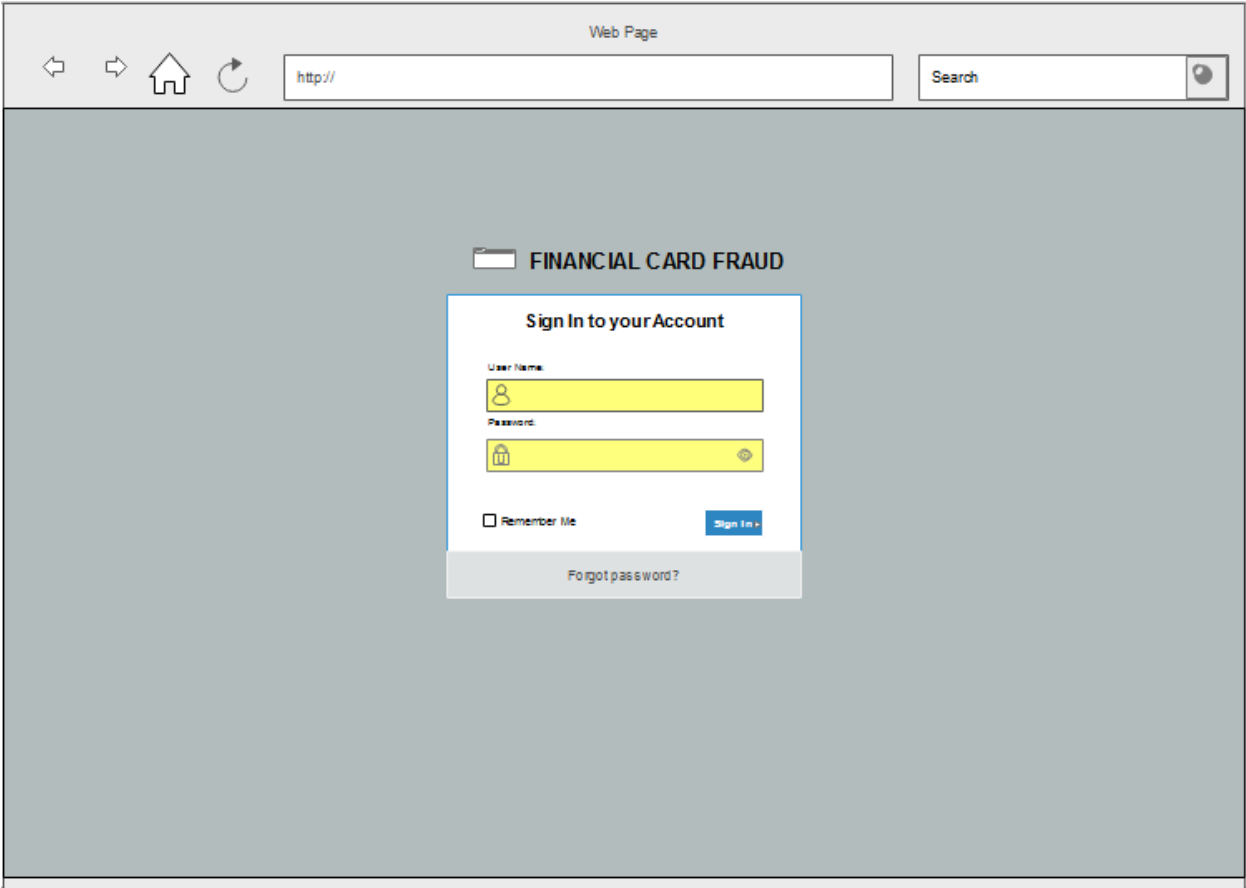
Appendices

Appendix A: Wireframes

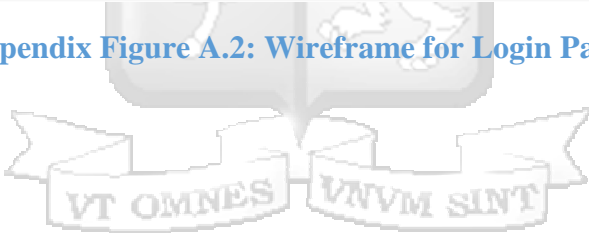


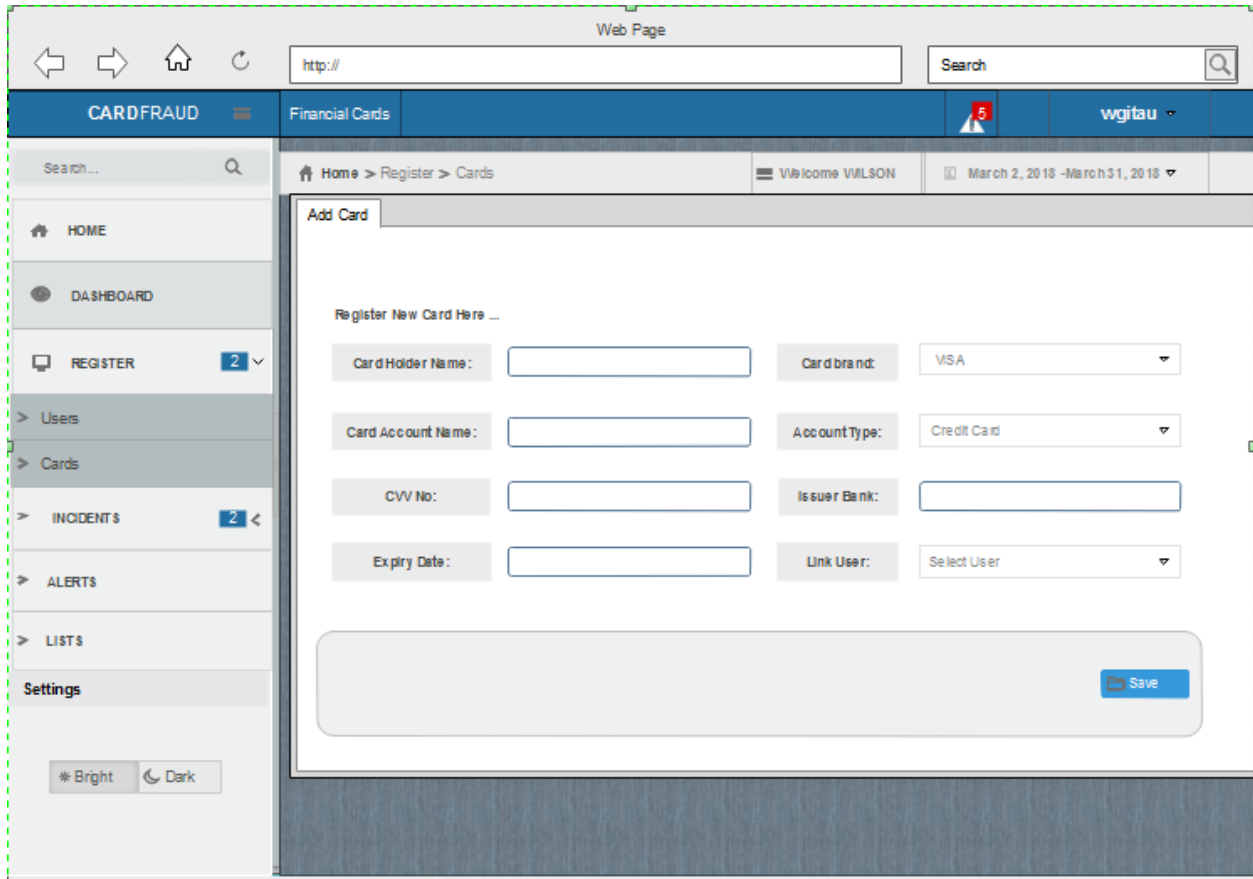
Appendix Figure A.1: Wireframe for User Registration



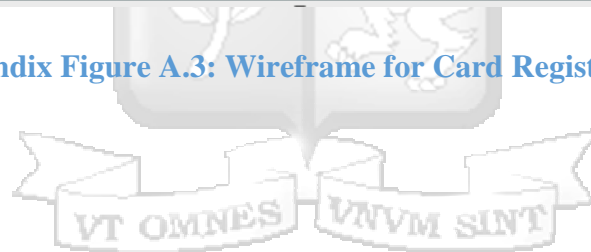


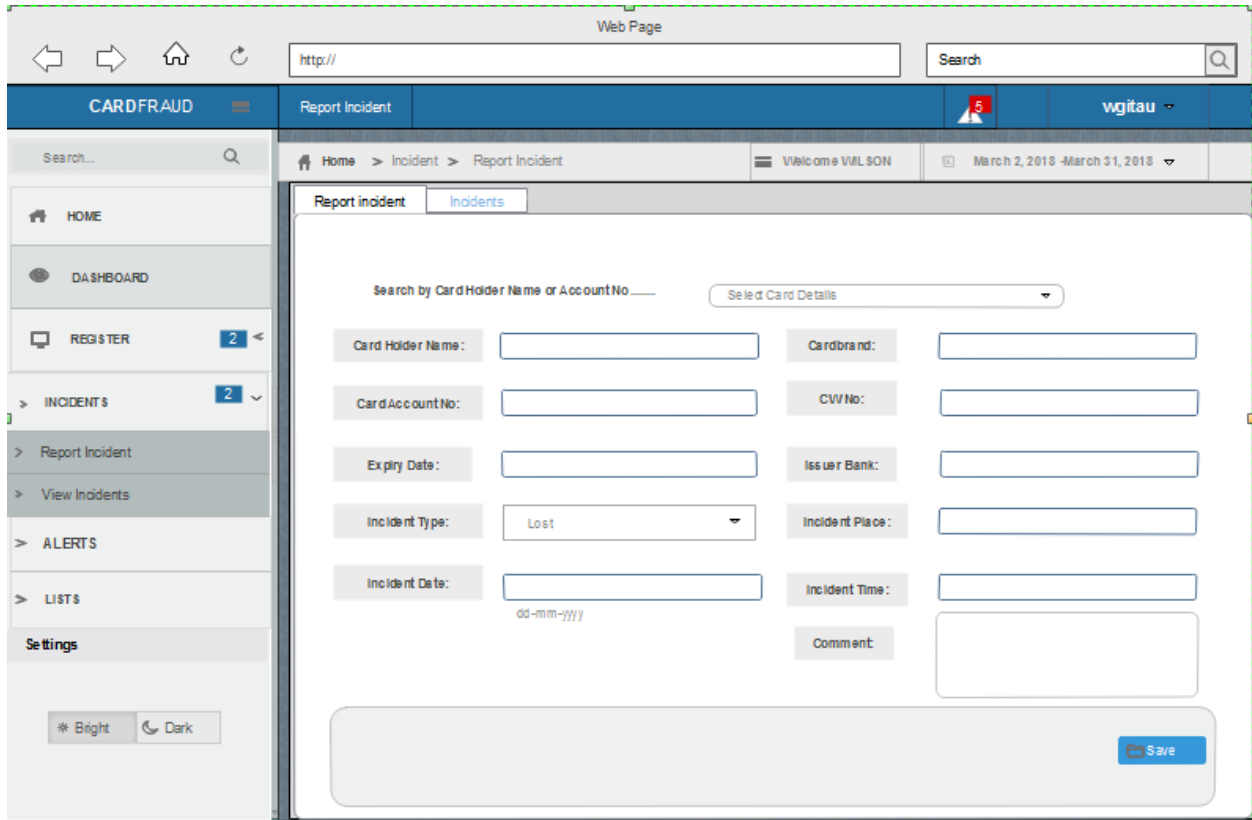
Appendix Figure A.2: Wireframe for Login Page



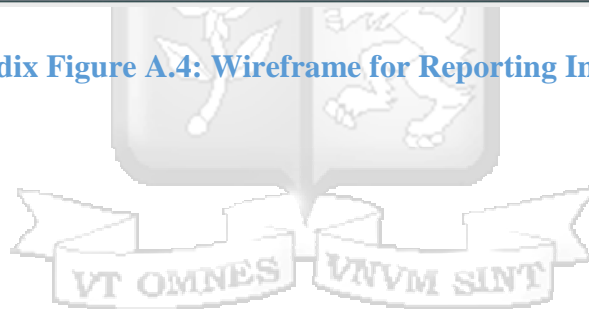


Appendix Figure A.3: Wireframe for Card Registration





Appendix Figure A.4: Wireframe for Reporting Incidents



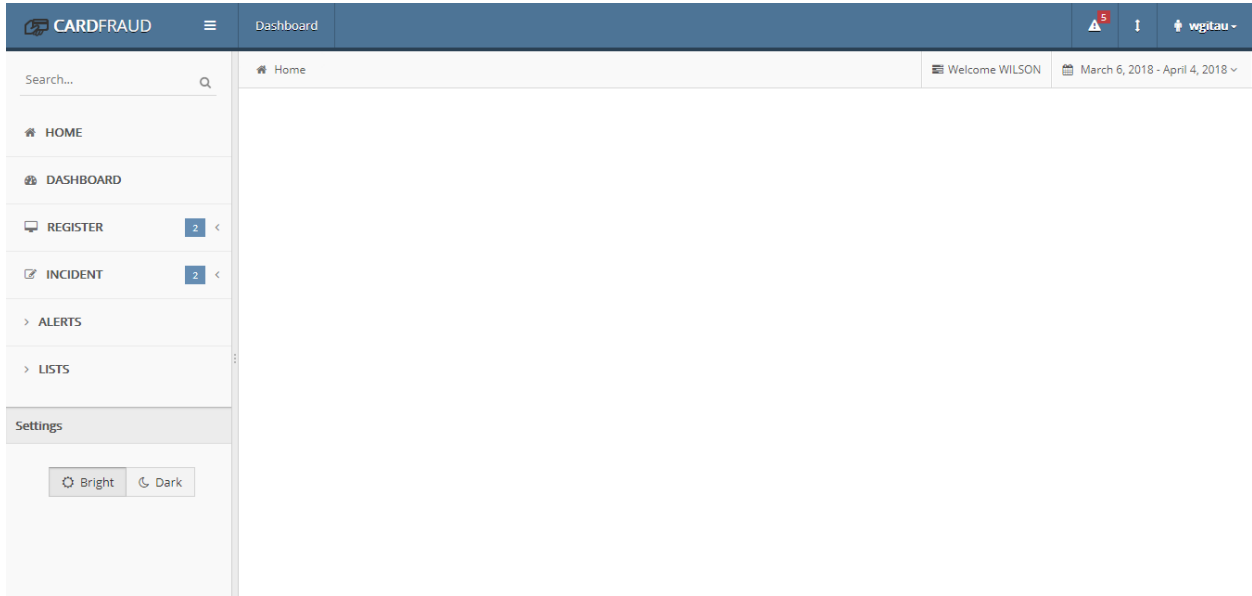
Appendix B: Screenshots

The screenshot shows the 'CARDFRAUD' application interface. The top navigation bar includes the logo, a menu icon, the current page 'Users', a notification bell with '5', a user profile icon for 'wgitau', and a date range 'March 6, 2018 - April 4, 2018'. A left sidebar contains navigation options: HOME, DASHBOARD, REGISTER (with a '2' badge), Users (highlighted with a blue box), Cards, INCIDENT (with a '2' badge), ALERTS, and LISTS. Below the sidebar are 'Settings' and 'Bright/Dark' mode toggles. The main content area is titled 'New User' and contains a registration form with the following fields: First Name, Middle Name, Surname, Username, Email, Stakeholder (a dropdown menu currently set to 'Individual'), Country (a dropdown menu currently set to 'Select Country'), Id /Business No., and Tel No. A blue 'Save' button is located at the bottom right of the form.

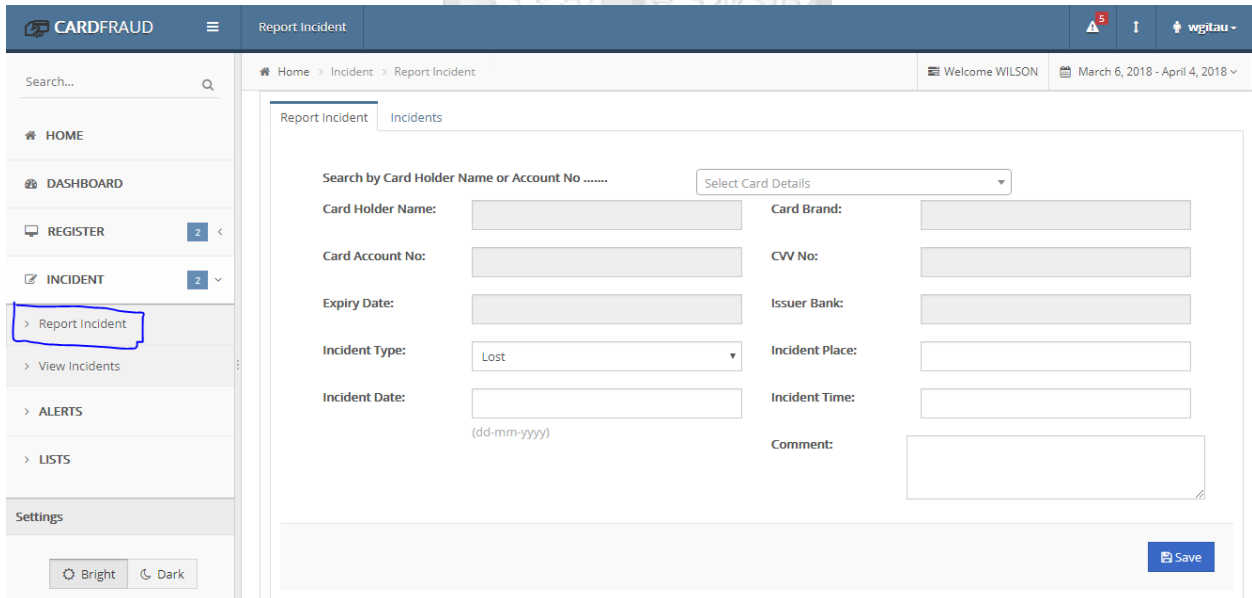
Appendix Figure B.1: Shows the User Registration Form

The screenshot displays a login form overlaid on a background image. The background features a hand holding a credit card, with text elements including 'FINANCIAL CARD FRAUD', 'Credit card protection', 'FRAUD PREVENTION', 'Identity protection', and 'Data protection'. The login form itself has a title 'Sign In to your Account' and contains two input fields: one for the username 'wgitau' and one for a masked password '.....'. Below the password field is a 'Remember me' checkbox and a blue 'Sign In >' button. At the bottom of the form is a 'Forgot Password?' link. A link for 'Don't have an account yet? Sign Up' is also visible at the bottom of the background image.

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

Home > Incident > Report Incident Welcome WILSON March 6, 2018 - April 4, 2018

Report Incident Incidents

Search by Card Holder Name or Account No WILSON GITAU-345677664678-VISA Blacklist Card

Card Holder Name:	WILSON GITAU	Card Brand:	VISA
Card Account No:	345677664678	CVV No:	456
Expiry Date:	2020-05-02	Issuer Bank:	EQUITY BANK

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

Home > Incident > Report Incident Welcome WILSON March 6, 2018 - April 4, 2018

Report Incident Incidents

Search by Card Holder Name or Account No RDFDSRCTYG-564767-VISA Healthy Card

Card Holder Name:	RDFDSRCTYG	Card Brand:	VISA
Card Account No:	564767	CVV No:	7678
Expiry Date:	2018-08-04	Issuer Bank:	rteytf

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

Appendix C: Application Interfaces

The screenshot shows a REST client interface with a sidebar on the left containing a 'History' tab and a list of recent POST requests to the endpoint `http://localhost/CardFraudBackend/configurations/QueryBlacklist`. The main panel displays a POST request to `http://localhost/CardFraudBackend/configurations/QueryBlacklist` with the following parameters:

Key	Value	Description
<input checked="" type="checkbox"/> card_holder_name	WILSON NDUNGI GITAU	
<input checked="" type="checkbox"/> brand	VISA	
<input checked="" type="checkbox"/> account_no	4567987667892643	
<input checked="" type="checkbox"/> cv_no	789	
<input checked="" type="checkbox"/> expire_date	2018-01-09	
<input checked="" type="checkbox"/> type	STATUS	
<input checked="" type="checkbox"/> user	wgitau	
<input checked="" type="checkbox"/> ip_address	172.89.56.87	
<input checked="" type="checkbox"/> zip_code	00900	
<input checked="" type="checkbox"/> state	Washington	
<input checked="" type="checkbox"/> telephone	+2567865444567	
<input checked="" type="checkbox"/> name	james bond	
<input checked="" type="checkbox"/> info	purchase of a goods	
<input checked="" type="checkbox"/> email	edmn@capital.com	

The interface also shows a 'Send' button and a status bar indicating 'Status: 200 OK'.

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

The screenshot shows a REST client interface with a sidebar on the left containing a 'History' tab and a list of recent POST requests to the endpoint `http://localhost/CardFraudBackend/configurations/Alerts`. The main panel displays a POST request to `http://localhost/CardFraudBackend/configurations/Alerts` with the following parameters:

Key	Value	Description
<input checked="" type="checkbox"/> user	wgitau	
<input checked="" type="checkbox"/> ip_address	172.89.56.87	
<input checked="" type="checkbox"/> zip_code	00900	
<input checked="" type="checkbox"/> state	Washington	
<input checked="" type="checkbox"/> telephone	+2567865444567	
<input checked="" type="checkbox"/> name	james bond	
<input checked="" type="checkbox"/> info	purchase of a goods	
<input checked="" type="checkbox"/> email	edmn@capital.com	
<input checked="" type="checkbox"/> type	ALERTS	

The interface also shows a 'Send' button and a 'Save' button. The status bar indicates 'Status: 200 OK' and 'Time: 255 ms'.

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

```
1 {
2   "body": "Successfully Sent",
3   "status_code": 200
4 }
```

Status: 200 OK Time: 255 ms

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

POST http://localhost/CardFraudBackend/configurations/QueryDetails Params Send Save

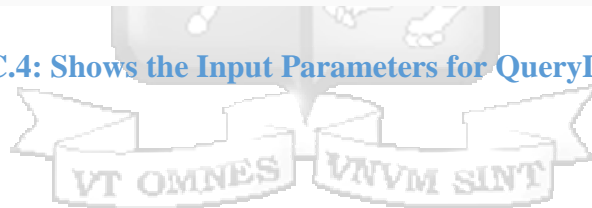
Authorization Headers Body Pre-request Script Tests Code

form-data x-www-form-urlencoded raw binary

Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/> card_holder_name	WILSON NDUNGI GITAU			
<input checked="" type="checkbox"/> brand	VISA			
<input checked="" type="checkbox"/> account_no	4567987667892643			
<input checked="" type="checkbox"/> cv_no	789			
<input checked="" type="checkbox"/> expire_date	2018-01-09			
<input checked="" type="checkbox"/> type	STATUSINFO			
New key	Value	Description		

Body Cookies Headers (9) Test Results Status: 200 OK Time: 335 ms

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



Appendix D: Turn it-in Report

feedback studio Wilson Ndungi Gitau | Dissertation

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.

Match Overview

11%

Rank	Source	Match Percentage
1	Submitted to Strathmor... Student Paper	3%
2	etd.aau.edu.et Internet Source	1%
3	ucpd.berkeley.edu Internet Source	1%
4	ww2.klatu.net Internet Source	<1%
5	www.redlockslocksmit... Internet Source	<1%
6	Submitted to Wawasan... Student Paper	<1%

Appendix Figure D.1: Turnitin Report

