Regent Journal of Business and Technology 2024, 1(1): 1-30
DOI: 10.5923/j.rjbt.20240101.01

An Investigation into the Utilization and Integration of Digital Payments Schemes Using ISO 8583 Standard to Promote Cashless Payments in Zambia

David Kabulubulu Chanda*, Simon Tembo

Department of Electrical and Electronic Engineering, School of Engineering, University of Zambia, Zambia

Abstract Despite strides in payments technology, use of cash in consumer payments was prevalent in Zambia. In addition to other factors, the main factor for this low adoption of digital payments was lack of integrated payment schemes. In attempt to bridge this identified gap, the aim of this research was to find means of utilizing digital payments in consumer payments by trying to define an integration model for payment schemes using ISO 8583 standard. ISO 8583, 1993 was chosen to leverage on existing infrastructure available for all payments schemes to use at the Zambia Electronic Clearing House. The model would include technical and operational aspects that would facilitate use of digital payments by the three major take holders, being payment companies, merchants and consumers. Three baseline studies were conducted on each category of stakeholder using both quantitative and qualitative methods. Inferences from the studies were used in formulating an integration model by defining both technical and operational integration aspects. Technical definition involved redefinition of message flows, data fields and data fields population rules for the ISO 8583 MTI messages. The model was tested and validated by developing prototype acquirer and issuer interfaces that processed ISO 8583 messages, and neaPay ISO8583 processing simulator switch from neaPay Payment Solutions, representing the interconnecting switch at NFS. The developed model demonstrated that introduction of a central integration point would stimulate cashless payments, as it created an ecosystem which could address all stakeholder pertinent issues preventing utilization, such as security, cost and profitability.

Keywords Digital payment scheme integration, ISO 8583 customization, NFS E-Money, Cashless payments

1. Introduction

Digital payments involve the electronic transfer of cash from one party to another using a payment platform such as mobile banking, Internet banking or credit/debit card [8]. The platforms are facilitated by a payments company or scheme such as VISA, MasterCard, Zambia National Financial Switch, Commercial Banks, FinTechs, MNOs and the like.

The research investigated the current utilization of existing digital payments schemes in Zambia to make consumer payments as well as the how several existing closed loop digital payment schemes may be integrated using ISO 8583 standard by leveraging on existing infrastructure that already supported the ISO 8583stadard at the Zambia Electronic Clearing House Limited (ZECHL) under the National Financial Switch (NFS).

The years leading to 2022 had witnessed dramatic changes in the payments industry with the rise in digital payments worldwide. These changes are accelerating as more people around the world use contactless cards and smartphones to pay each day transforming the face of commerce as not just every person, but every device that a person interacts with, becomes a commerce opportunity [1] [2] [3]. Zambia has not been left out in this rise in digital payments innovations which has recently been further fuelled by the outbreak of the Covid-19 pandemic.

However, despite this rise in electronic payment solutions, the use of cash in consumer payments is still dominant [2]. According to a research by ZICTA, in Zambia, only 25.4% of total population had access to mobile telephones in 2014, this number rose to 53% in 2018. This increase in access to mobile phones reflects the increase in digital payments as most of digital payments are performed through mobile telephones. However, as depicted in Figure 1.., this increase is mainly around peer to peer transfers as opposed to consumer payments. By deduction, this means that most of consumer payments in Zambia were performed by cash [6].

The dominance of cash payments was also backed up by another report of the Bank of Zambia, according to which, for the first half of 2019, debit card holders had withdrawn about 23 billion kwacha from ATM cash points, but had only transacted for about 9 billion kwacha on electronic

* Corresponding author:
kabulubulu.c.d@gmail.com (David Kabulubulu Chanda)
Received: Dec. 26, 2023; Accepted: Jan. 12, 2024; Published: Jan. 15, 2024
Published online at http://journal.sapub.org/rjbt

POS devices [5] [7].

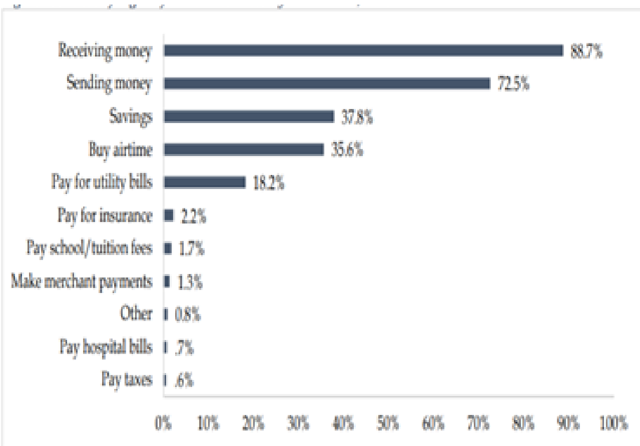

Figure 1. Usage of Financial Services by individuals

Several factors have been attributed to why there has been little diffusion in digital payments for consumer payments; these range from costs, phobia of technology and greatly to the lack of integrated infrastructure that support consumer payments. In Zambia, there were too many closed loop payment systems which had not leveraged on consumer payments, but had largely supported peer to peer transfers. Figure 2.., depicts the current closed loop payment schemes available, if these closed loop payments systems were integrated using a common standard, the adoption of digital payments for consumer payments may be improved.

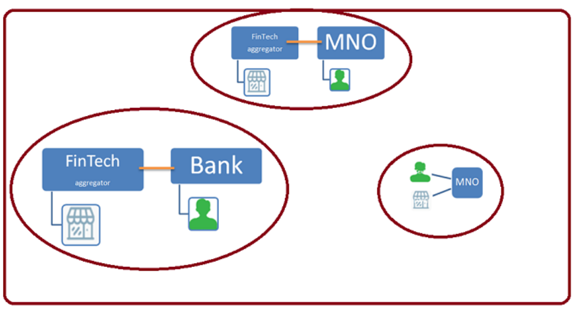

Figure 2. Closed loop payment schemes depiction

From the presented gap in lack of utilization of digital payment schemes largely attributed to the existence of too many closed loop payment schemes, the aim of this research was twofold: firstly, to identify means of utilizing the contemporary developments in digital payments technologies in reducing the use of cash in payments for consumer related transactions and secondly, to define a model and business process for integration of the various digital payments schemes in Zambia using ISO 8583 financial transactions standard.

2. Literature Review

2.1. Generic Digital Payments Ecosystem in Zambia

According to UNCDF and Bank of Zambia [7] [19], Zambia's payment landscape may be grouped into two categories, the critical stakeholders that form the backbone of payments in Zambia, and the mushrooming FinTechs playing a pivotal role in innovation but who's success depends on how they partner with the critical stake holders. Fig 2-4 shows some examples of the two categories.

Figure 3. Fintech Landscape in Zambia

Critical sate holders may be put into three groups, the Banks and Microfinance Institutions (MFI), the MNOs comprising of the three mobile network operators in Zamtel, Airtel Zambia and MTN Zambia. Lastly we have regulatory institutions, the major ones being the Bank of Zambia (BOZ), ZICTA, PACRA and a few more. Not depicted in the two figures but playing a major role, are the payment companies interconnecting the participants. These major payment companies include the National Financial Switch (NFS) at ZECHL, Visa and MasterCard. The latter three are mainly supporting debit card based solutions, but due to changing times have evolved into generic payments solution companies and have offered non card based payment options [7] [19].

2.1.1. Digital Payments Model (Debit Card Based)

When it comes to consumer payments, the foregoing stakeholders facilitate payments using models that generally interconnects a seller and a buyer. Several models exist that depict the payments ecosystem by categorizing the stake holders by the roles they play in the ecosystem. One common model derived from the debit/credit card payments systems as in figure 4 is commonly used. The model categorizes the core players in the payment transaction. Each payment transaction has a Payer and a Payee, where the payer has to transfer funds digitally to the Payee. This transfer of funds is facilitated by a payments company that connects the payer's platform to the payee's platform. For the ultimate settlement or transfer of funds, there is at minimum a bank to facilitate the actual movement of funds from the Payer's bank to the Payees bank. Figure 4 shows how the different players sit in the payments model. The model is applicable to any digital payments scheme, even away from debit/credit card schemes [8] [20] [21].

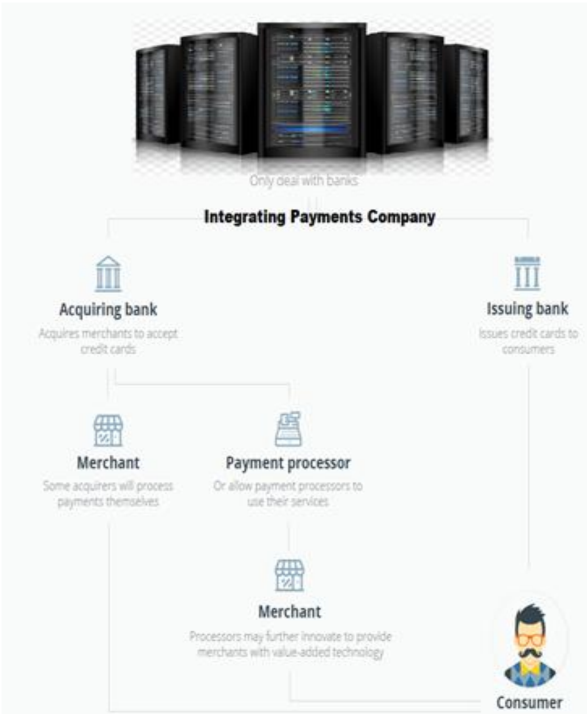

Figure 4. The Debit Cards payments model

2.2. Integration of Payment Schemes and the N-Squared Scalability Problem

In Zambia, there are several payments companies most of which are operating as closed loop systems, i.e. not interconnected to each other. Based on the premise that the more the integrations the higher the adoption of digital payments, each payment scheme may have to have interconnection with a significant number of other payment schemes. This however, introduces the N-squared problem. This means that for absolute interconnections, the number of interconnections would grow on the order of N-squared, with N being number of payment schemes in this case. A single interconnection point solves this problem.

2.2.1. Application Programing Interfaces (APIs)

Integrations involve the interconnection of different payment scheme software via API's or ISO standards. The APIs may be SOAP of RESTful. Many digital payment solutions have adopted RESTful web services as they are lightweight, flexible and efficient. Integrations are also achieved via several ISO defined interconnection standards such as ISO 20022 and ISO 8583. ISO 20022 is the newer version and has superiority functions over the order ISO8583. However, In Zambia, ISO 8583 enjoys widespread use and available infrastructure at ZECHL under the NFS. However, the standard would need customization of the data fields and message flow to meet the non-card based usage in consumer payments [12] [13].

ISO 8583 is a standard for systems that exchange electronic transactions made by cardholders using payment plastic cards. An ISO 8583 message is made of Message type indicator (MTI), One or more bitmaps, indicating which data elements are present and the actual data elements, the fields of the message as in figure 4 [14] [17] [18].

MTI	Bit Maps	Data Elements

Figure 5. ISO8583 Message Structure

Though originally developed and used by card based systems, the standard has been adopted by non-card physical based payment gateways and digital wallets. This mainly started with the introduction of e-commerce platforms. Payment gateway schemes such as VISA and MaterCard who originally supported card based transactions were forced to evolve to support new payment options that did not require a card to be present, these payment options are generally referred to as Card Not Present (CNP) type of transactions [14] [15] [16].

2.3. Factors in Payments Systems Integration

In addition to the N-squared problem, empirical research has revealed several reasons as to why payment schemes may be having operating in silo as detailed below;

2.3.1. Standards, Models and Architectures

Different payments systems are developed using different standards, models and architectures, this presents a challenge when two systems of different architectures try to interconnect. For the systems to connect, an integrating model would have to be developed which should encompass all aspects of integration including what standard to follow (API or ISO), model for systems interconnection, allocation of tasks and responsibilities, architectures, how settlements would be done, pricing models, dispute resolution and ultimately conformity to regulation. [23].

2.3.2. Security

Security is a major factor in any integration that would be there, it may be a determining factor as to whether a payment system is willing to interconnect to another. For example, for participants in the debit card industry, any new entrant will have to undergo Payment Card Industry Data Security Standards (PCIDSS) certification before they are allowed onto the network. Payment systems like Visa and Mastercard will not accept any new entrant without a PCDISS certification. Regulators find it hard to balance between rapid acceptance of new technologies on the market and making sure that each one of those players is compliant to the best security practices. Stringent security requirements may hinder small but innovative players [22] [24].

2.3.3. Profitability

Integration in many case comes with costs, any institution looking to integrate with another will definitely consider the profitability of the venture. The benefits may be the direct income charged to the users of the system or inform of intangible benefit that may lie in the users' experience. A system that is interconnected is generally widely used and hence perceived to be reliable and established, this good reputation does profit the payments company in many ways.

2.3.4 Regulation

Regulation is always at the centre of any financial system. Most governments foster financial inclusion by regulating how the financial industry works. For example, in Zambia, the government through BOZ and Zambia Electronic Clearing house introduced the National Financial Switch (NFS) and directed all banks to route all local debit card transactions through this switch [5] [7] [25].

2.4. Utilization by Merchants and Consumers

Research on utilization of payment technologies, sometimes referred to as diffusion or acceptance of innovation, has been based on several common theories which include Diffusion of Innovation theory, Theories of Reasoned Action and Theories of planned Behaviour (TRA/TPB), Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). The theories speak to either the rate at which innovation is utilized [10]. or the underlying behavioural intentions to use or not use technology [10] [11]. Empirically, According to a research by GSMA [26], there is an increase in smartphone adoption in emerging markets and a growing internet penetration that is fuelling the expansion of e-commerce. E-commerce has become a significant tool in unlocking job creation and innovation for small and medium-sized enterprises (SMEs) in developing countries. Further, the World Bank's Global Findex database shows that in key mobile money markets, e-commerce is being used by low-income and rural people. However, in these markets, over 70% of e-commerce payments involve cash-on-delivery payment processes, which are expensive, inefficient and time-consuming for both merchants and buyers [26] [27]. Several scholars' research using the above mentioned theories, have attributed the low uptake of digital payments around consumer payments to several factors as below.

2.4.1. Poor Digital Payment User Experience Results in High Drop-Offs

GSMA [9], discovered that users are often instructed to follow 8-10 step processes independently, and are forced to enter numerous details (merchant numbers, reference codes, amounts) precisely, creating multiple chances for error. In addition, drop-off points were also due to network failure, lags in sending the messages and expiration of the One Time Passwords (OTP). The factors extend to other forms of digital payments, for example according to a survey by visa [1], most debit card users found the checkout time lengthy, and a high network failure for most POS transactions in Zambia. These users tend to lose trust in the payment scheme and are more likely to carry cash as a backup or entirely doing away with the debit card payments all together. Poor user experience is not only limited to the payment aspect of the integration—the delivery and refund / exchange processes are also at the core of the online purchasing experience. Delivery in most emerging countries is typically slow and inefficient because of the poor address system in cities and lack of widespread reliable delivery services in non-urban areas for the case on online purchases were the customer buys in a non-brick and motor shop a expects the shop to deliver the product later. The refund / exchange process is also complex and lengthy, with customers often only being able to receive vouchers in place of a faulty or non-desired item.

2.4.2. Lack of Integration of Payment Schemes

According to the FinScope Zambia, 2015 research demographics [4], financial inclusion was over 50%. The study also showed that over 54.8% of Zambian adults live in rural areas. When we look at most integrated payment scheme in Zambia, the debit card network, it has very minimal rural penetration. Banks who are the primary provider of this service incur huge expenses in running ATM cash points in rural areas. This means the over 54.8% of financially included adults are accessing financial services via alternative payment schemes which are mostly closed loop. If a consumer and merchant are on two different payment scheme, the transaction cannot happen [5] [7].

2.4.3. Security

According to a study by Visa [1] on fraud, it showed that most customers that had experienced fraud directly or through a close relation tend to show less confidence in the digital payments schemes. Customers feel the systems are not secure enough and would rather carry cash for their consumer payments and/or peer to peer transfers. On the side of merchants, the merchant has a risk of paying for fraudulent transactions [5].

2.4.4. Cost

According to Ann Kjos [28], most merchants prefer cash because they feel accepting debit cards is expensive. In the debit card model, the merchants is charged for accepting a digital payment, the rationale is that the merchant saves in terms on handling cash and has instant or almost instant access to the money in their account and are able to utilize it quicker that if they had received cash which they had to first deposit into a bank account. Other than paying for accepting the terminal, the merchant is also charged for using the POS terminal, the merchant is also liable to fraudulent transactions.

2.4.5. Awareness

In a study by P. Ratan [8] on digital trends issues and opportunities, it was discovered that some consumers use cash simply because they are not aware that they can make a digital payment. This is a trend noticed even in a population that is fairly informed and savvy. Like in the case of the bank customers that had withdrawn 22 billion kwacha on the ATM in 2019, a good number might have not known that they were able to make payments with their card at various shops [5] [7].

2.4.6. Regulation and Policy

Regulation plays a pivotal role in the payments industry. Establishment and implementation of policy that promote digital payments can help increase the number of digital payments in country [5]. There are seral ways in which the government can stimulate digital payments including making cost of digital payments cheaper by reducing tax on digital payments technology such as ATMs, POS, software procurements, reduction of physical cash in circulation and fostering awareness and training to the general populace [25].

3. Methodology

3.1. Introduction

The generic methodology for the research was mixed methods research in which both quantitative and qualitative data were collected from three baseline studies.

3.2. Base Line Studies

Literature review exposed three main stakeholders in digital payment system integration and utilization namely the payment companies that facilitate the payments, the merchants that sale the goods or services and the consumers that buy the goods or services. To help in the development of the integrations model, baseline studies were conducted on each of the three categories to draw the much needed insights in the development of the integration model.

3.3. Payment Companies: Challenges Faced by Digital Payment Companies in Integration

3.3.1. Sampling

For this baseline study, purposive sampling was used to identify payment companies that facilitate digital payments. Homogenous purposive sampling was chosen because the researcher's focus was on particular characteristics of the population that were of interest to enable the researcher answer the research questions which were related to digital payments integration by the digital payment companies. Five digital payments service providers namely, Zambia Electronic Clearing House ZECHL, Indo Zambia Bank, Cgrate Zambia, Cellulant Zambia and Airtel Zambia were engaged in interviews, observation and collection of digital payments statistics. The institutions had been chosen to have representation from different types of digital payments service providers covered. ZECHL as pivotal as the integrating company that run a switch that's supports ISO 8583 integrations under the NFS.

3.3.2. Data Collection

For the purpose of determining the challenges faced by digital payments schemes in integration and understanding the current business processes in consumer digital payments; review of literature, interviews, and payments company observation were used. Review of literature helped the researcher frame purposive questions for interviews conducted with the digital payments companies. Interviews helped the researcher close gaps that would have been left out during the literature review process. Observation and study of the sampled stakeholders enriched understanding of the challenges faced by the payments companies. From the findings in purposive literature review, interview, observations and study of the digital payments companies, a digital payments integration model was designed, validated and critiqued. Tools used for the design and validation included neaPay payment solutions Issuer and Acquirer simulator and switch which supports ISO 8583 messages. A prototype interface which was able to pack messages to and unpack and parse messages from the neaPay ISO8583 simulator, was developed using PHP server side scripting language.

3.4. Adoption of Digital Payments by Sellers (Merchants) and Buyers (Consumers) Payments

3.4.1. Sampling

Merchants that accepted both cash and digital payment means were purposively sampled, similarly, consumers that had options of paying by cash or digitally were also purposively sampled. The population size for the number of merchants was established from BOZ report on digital payments [5] [7]. The report indicated that there were over 6,915 merchants accepting digital payment forms. The population size for number of consumers was established using the demographic findings of FinScope Zambia, a research conducted by Financial Services Deepening Zambia (FSD Zambia) on financial inclusion [4]. The research indicated that over 8.9 million Zambians were financially included and were able to make consumer payments. According to the World Bankv [32], Zambia's urban population by 2021 was 45% of total population.

However, homogenous purposive sampling was chosen for both categories of participants because the researcher's focus was to build on already established reasons for non-adoption from review of similar research to be used as insights in development of the integrating model using ISO 85833. The conveniently sampled participants were 50 merchants and 170 consumers.

3.4.2. Data Collection

Two sets of self-administered questionnaires were sent to the purposively sampled merchants and consumers via google docs forms. The contents of the questionnaires were guided by the findings in the literature review. Several adoption of technology theories were reviewed and their finding used to frame both closed ended and open ended questions to help in the development of a model that encourage the merchants to accept payments digitally as opposed to cash. The theoretical literature had indicated that the key independent variables that affect digital payments utilization are user experience, lack of integration, security, cost, awareness and regulation and policy. And hence the questionnaires tried to validate if this was a true reflection from Zambia's merchants and consumers.

3.4.3. Presentation

Descriptive statistical analysis technique was used to analyse the data obtained from the merchant's questionnaire. Qualitative data were analysed by patterns and trends that were categorized and interpreted in relation to how it influences the design of the integration model. These responses were grouped according to themes of the questions. Furthermore, quantitative data were analysed using SPSS. Descriptive statistics were applied to the processed data by showing variable frequency distributions from the responses obtained. Data were presented using graphs, charts, tables and percentages.

4. Results and Discussions

The aim of this research was find means of utilizing digital payments in consumer payments by trying to define an integration model for payment schemes using ISO 8583 standard. Three baseline studies were conducted.

4.1. Payment Companies: Challenges Faced by Digital Payment Companies in Integration

The objectives of this baseline study were to firstly find out if there were integration or interconnection of different payment networks in Zambia for consumer payments, secondly, to find out if ISO 8583 1993 standard could be used to interconnect several payment companies and finally to find out what challenges if any, are faced by the payment companies in integration process. The study implored qualitative method where five payment companies were interviewed, 63 BOZ designated payment companies observed and literature reviewed. The results are summarized in Table 1.

Table 1. Payment Company Integration Summary Results

Theme	Literature review	Interviewed Payment Companies	Observations of Most Payment Companies
Is there integration of digital payment schemes in Zambia?	The researcher could not find literature that directly addressed this question. The closest was the bank of Zambia Website which listed all designated payment companies but did not mention of their interconnections [5] [7].	Key project managers and personnel of selected five institutions confirmed having at least one integration, however, for most of the institutions this single integration was with a bank but no other wallets and was mainly for peer to peer transfers	The researcher probed other payment companies, with 63 payment companies and found that few had integration with more than 10 other payment companies. It was noted that for payments, some merchants (e.g. government sites) had to onboard more than once payment company to give their customers options.
Can several digital payments schemes be integrated using the ISO 8583 1993 financial transactions standard?	ISO 8583 has been used by card schemes such as Visa and MasterCard to process card not present (CNP) transactions commonly known as E-commerce [14]. While these mainly revolve around sending virtual card data, there has been extended usage via API integrations to act as a gateway [16]. At world level, top digital wallets like Apple Pay, Samsung Pay, PayPal and Alipay are able to move funds to and fro their wallets via ISO8583 customizations [17] [18]	It was discovered that ZECHL had actually started a similar project allowing MNOs to connect to the NFS via ISO 8583. However, there seemed to be issues around message flow definition that potentially would cause financial loss to participants in cases of lost messages. Most interviewed project managers had Engaged BOZ and ZECHL to join the NFS for this service. From Specification documents [33] [34] shared, this interconnection only defined transfers, cashout and cash in use cases, there was no payment use case defined.	Most Zambian Wallets and Payments companies seemed to draw inspiration from international wallets like Apple Pay and PayPal, their use cases were identical in most cases. From this observation, the researcher concluded their architecture could be scalable enough to integrate to the NFS using ISO 8583
What challenges are faced by digital payments companies in integration of their payments schemes to other companies' payment schemes?	Security, Regulation [1] [2], Project profitability [29] [30], lack of unified interoperability standards [24] and Operational Risks [3] as the major challenges faced by payment companies when integrating	Most of the project managers, and key project personnel interviewed stressed on the challenges of managing multiple interfaces. Most stressed on issues to do with Regulation, Operational Risks, Security, Costs and general Operational challenges.	It was also noted that that Settlement risk and repeated fraud incidents on some named companies were a major blocking factor when it came to integrations.

4.1.1. Summary

This base line study answered the survey questions. There was little integration of payment companies in Zambia, ISO 8583 can be used to bring about integrations and there were challenges around integration that needed to be considered for any defined integration model. These findings were used in the customization of the ISO 8583.

4.2. Adoption of digital Payments by Sellers (Merchants) and Buyers (Consumers) Payments

The main goal of these two baseline studies were to find out why there was little adoption of digital payments by the merchants and consumers despite them currently having options to utilize the same.

4.2.1. Why do Merchants Accept Cash Payments in Zambia

Several surveys around technology acceptance models indicated that the intention to use or not use a payment technology where based on perceptions such as cost, convenience and past experience [11]. The merchants were given canned responses based on these suggestions from literature review. It however turned out that the major factor, accounting for 31% of responses was the willingness of the consumers to pay electronically. Other factors still remains relatively prevalent such as perceptions on cost, and generally how the merchant's payment operations are handled by their payment network. One notable deviation from what literature had suggested in [11] was that payments companies were not aware of electronic payments or that it was difficult to work with such payments. The results indicated otherwise. However, the latter may also be the concentration risk of homogenous sampling as Hutchinson [31] puts it where the sample responses may not represent the entire population.

4.2.2. Reasons for Cash Payments by Consumers

Cash payments are predominant, from results of this baseline study the major reason was that it was the only option given by the merchant. This is supported by the fact that there was less integration, hence most merchants, especially the small business, would prefer receiving cash as it is expected that most consumers would be able to pay by cash. The issue of cost was also a major factor, consumers are charged when paying cashless and this results in most preferring cash. Contrary to the literature, the results showed that awareness was not a major problem, this can be backed up by the fact that recent years have seen many digital payment options being developed and advertised by established companies such as Visa and MasterCard [1] [2].

4.2.3. Summary

The two baseline studies gave some valuable insights as to why merchants and consumers prefer cash as opposed to electronic payments. The reasons suggested by literature review where to some extent affecting merchants and consumers' decision in utilization of digital payments, however, slight deviations were noticed, for example, awareness was not really a factor as suggested by literature review.

The insights were incorporated in the operational aspects if the developed model. These operational aspects speak to cost for consumers and merchants, how quickly merchants account get credited and dispute resolution timeframes.

4.3. Development of the Digital Payments Integrations Model

The inferences drawn from the three baseline studies were used to develop the integration model. It was observed that Zambia had a National Financial Switch (NFS) at the Zambia Electronic Clearing House (ZECHL) that was supporting debit card payments, but could be leveraged on to support non card originated transactions by modifying the Data Fields and the Message flow of the ISO 8583 message standard. This led to the definition of the payment use cases to be supported, then redefining the necessary data fields of the ISO 8583 message to support the use cases then finally defining message flow to carter for network failures and lost messages. A prototype interface was developed using PHP, the interface was able to pack an ISO 8585 message and transmit it to the neaPay switch, which sent back a response to be unpacked and parsed by the proto type interface.

4.4. Current Business Process in Digital Payment Integration

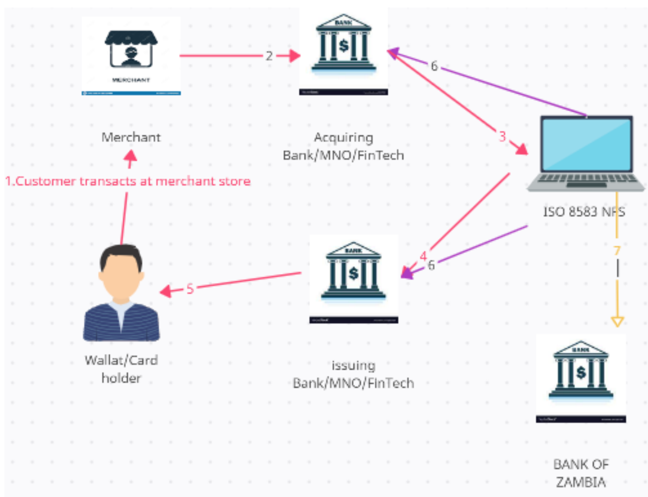

Figure 6. Debit Card Ecosystem business process in Zambia

In the current card network as depicted in Figure 6, transaction processing is in three stages.

1. **Transaction Authorization (1-5):** in this stage, a consumer makes a payment at a store by presenting their debit card to the merchant. The merchant reads card data and generates an ISO authorization message to the NFS, the NFS uses the data fields to route the transaction to the card issue who authorizes the transaction and sends a response to the merchant through the same channel. This happens online.
2. **Clearing (6):** In this stage, at the end of the business

day, the NFS aggregates transactions and comes up with net positions for each participant. This stage is offline. They then share the summary and detailed report files with the participants via Secure File Transfer Protocol (SFTP).

3. **Settlement (7):** The NFS then sends settlement instructions to the Bank of Zambia (BOZ) to debit or credit a participant. It's worthy to note that non-Bank participants, are not allowed to have an account at BOZ, and hence would have to find a sponsor bank which will be receiving settlements on their behalf.

4.5. Current Implementation (NFS E-Money) with Financial Exposure Challenges

Engagement with the ZECHL had revealed that ZECHL [33] [34] had started a similar project of interconnecting MNO, Fintech and Bank wallets using ISO 8583 using the architecture depicted in Figure 7. However, their use cases were currently limited to transfers, deposits and withdrawals as opposed to consumer payments, and introduced financial loss to the participants when a transaction message is lost.

The financial loss is because traditionally, ISO 8583 allows the authorizing party (issuer) to debit their customer and await settlement as opposed to crediting the customer then await settlement. When there are timeouts or dropped messages, the issuer faces financial loss risk as they would have to recover from the customer, hopping the customer would still have funds.

Figure 7 shows the message flow for all transfer use cases and the cash in use case alluded to earlier. The acquirer then sends a balance enquiry to the issuer as depicted by message 1 to 4 in figure above. The ISO8583 balance enquiry message returns the receivers Know Your Customer (KYC) details, simply put, their name and address. This gives chance to the sender to confirm they are about to send funds to the intended recipient.

The acquirer then sends an ISO 8583 full financial (1200) to the issuer as depicted in messages 5 to 8 . If the receiver's account in the financial message is correct and there is no restriction on the account, the Issuer debits a suspense account and credits the receiver the value in the message. It is important to note that at this point, the issuer is out of pocket and would expect that the NFS will debit the acquirer and credit them the next day. If the response in message 7 is approval, the NFS will mark this transaction for settlement in which the acquirer would be debited and the Issuer credited. It is also worthy note here that the acquirer would have excess at this stage and would expect that the NFS will debit them and credit the issuer the next working day. This flow works perfectly in real time when there are no lost messages or technical challenges at any one point from messages 1 to 8.

However, lost messages and technical challenges at any one of the 8 stages are eminent and the system has to recover from such. If the failure is at any of the stages from 5 to 8, the acquirer sends a reversal message MTI (1400). With this message the NFS and issuer are supposed to negate any action taken if they had received the original MTI 1200 message or ignore if they cannot find the original 1200 financial message. Again this works if the failure is at 5 and 6, if failure is at 7 or 8, two dangerous scenarios arise as in figure 8 and figure 9.

Failure at message 7: If there is failure at message 7, the issuer would not know about it until after clearing files are shared which happens next day. This is because the NFS would send a timeout or issuer switch inoperative response to the acquirer and no reversal would be generated. Further the NFS would not mark this transaction for settlement as it would not have received approval. This puts the issuer in financial loss risk if the customer utilizes the funds before clearing files are shared and the issuer performing reconciliation. Recovery of funds may not be guaranteed as it also leaves room for deliberate blocking of outbound response by a fraudulent insider with intentions of defrauding the issuer.

Failure at message 8: If there is failure at message 8 and message 7 was an approval response, the NFS would have marked the transaction for settlement while the acquirer would time-out and generate a reversal. The acquirer would not debit the senders wallet but the NFS would debit them at settlement putting them in a loss position. However, the reversal is supposed to negate this. If the reversal message does not get lost at any point, both the NFS and issuer are supposed to accept the reversal and negate the previous action which is unmark for settlement for the NFS and debit receiver and credit suspense for the issuer. This only happens if they are able to look up the original 1200 message, if the previous message is not found, the 1400 reversal message is ignored.

While the reversal sorts out the problem of lost message at 8, it is not guaranteed that the issuer would be able to successfully reverse funds from the customer because even latency or seconds, the receiver may utilize the funds leaving the acquirer in a loss position.

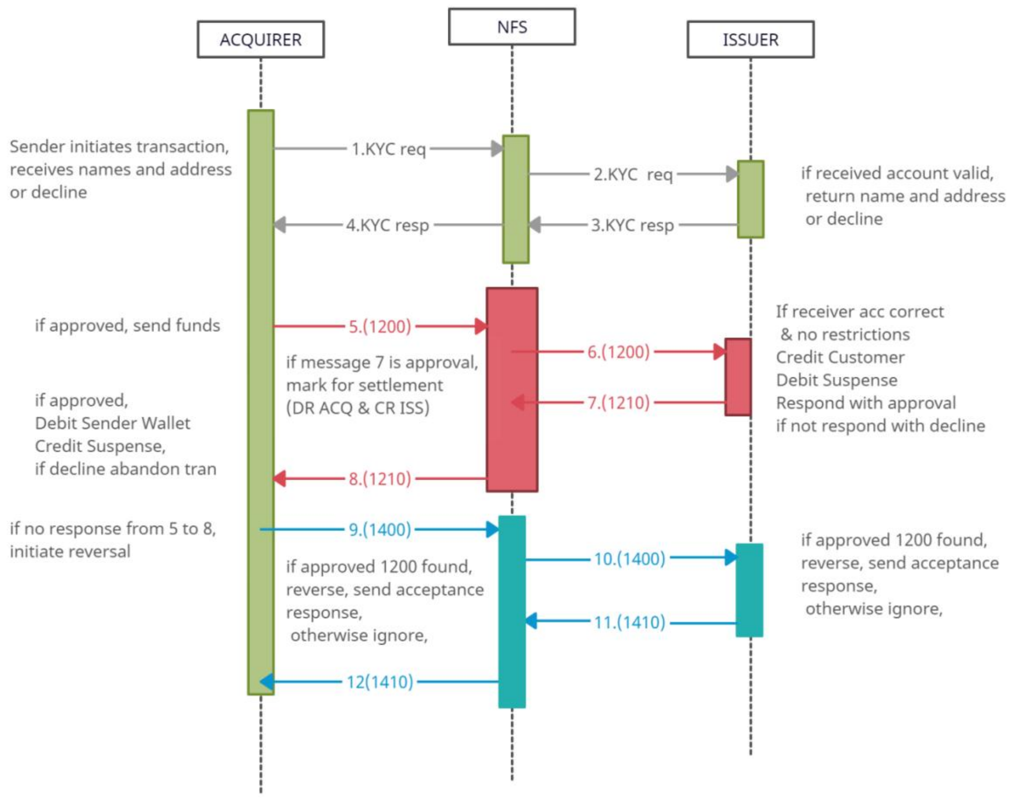

Figure 7. Current Message Flow (Transfers and Cash-in)

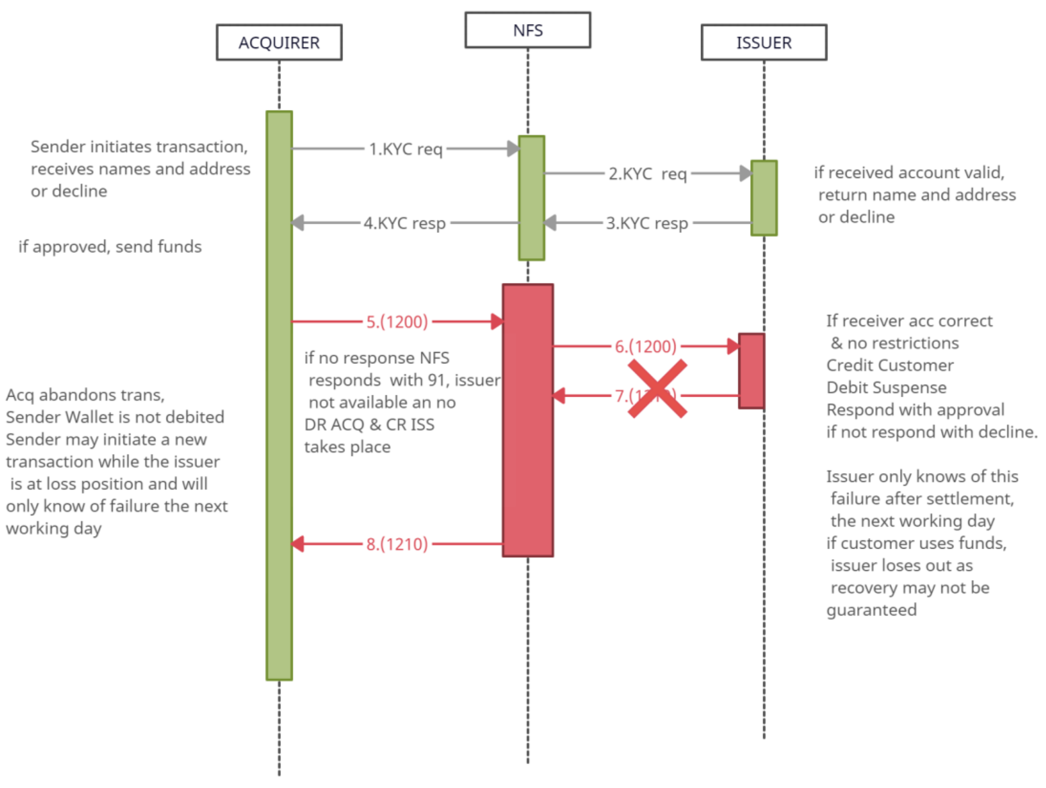

Figure 8. Failure at message 7

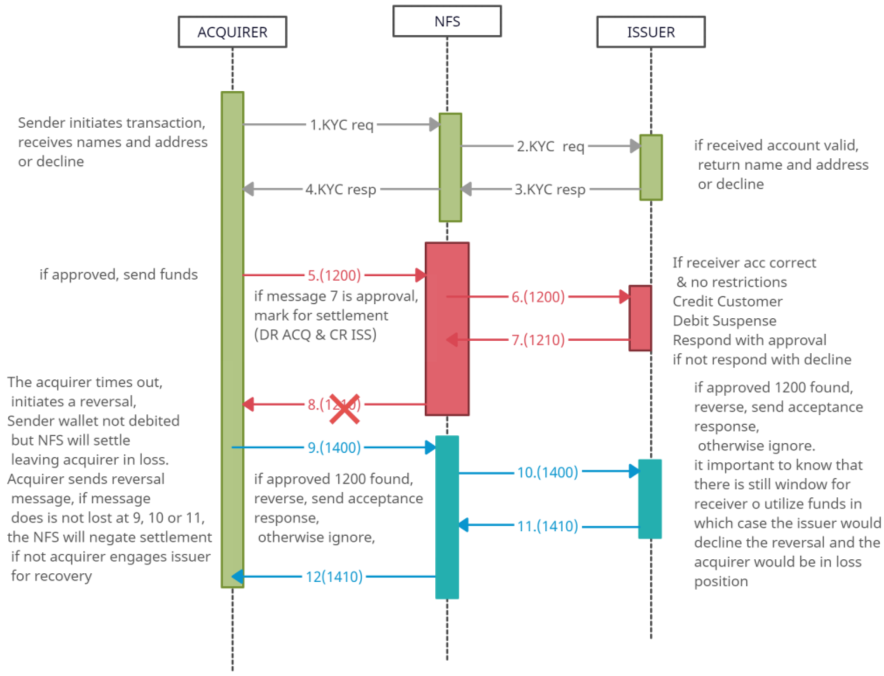

Figure 9. Failure at 8

4.6. Proposed Integration Model

4.6.1. Message Flow Customization

In the customization of ISO 8583 fields the acquirer and issuer shall be defined as follows.

Acquirer: This shall be the initiator of the transaction, will stand in for the buyer (consumer). The acquirer will be debited at settlement.

Issuer: This shall be the party that responds to the acquirer initiated message and will stand in for the seller (merchant). The issuer shall be credited at settlement.

The proposed architecture involved changing the current message flow as depicted in Figure 7 to accommodate for lost messages without exposing any participant to financial losses.

This involved the introduction of an ISO 8583 authorization message (1100) after the KYC message as depicted in Figure 10. The purpose of the authorization message was to allow the issuer credit the receiver with un-cleared effect, that is the receiver does not have access to the money at this point. The issuer then proceeds to respond to the authorization message with an approval. Upon receipt of approval of the authorization message, the acquirer can debit the sender wallet and credit a suspense account then proceeds to send a financial message 1200 and awaits response. The NFS shall use the incoming 1200 from acquirer to mark for settlement (Debit acquirer and Credit Issuer) and forward the 1200 to the issuer. The issuer uses the 1200 to make the earlier credit to receiver available for use, and sends acceptance response to the acquirer. The response to acquirer is basically advisory and would not prompt any action by the NFS nor the acquirer in terms of debits to the sender and acquirer respectively.

If any of the messages from 9 to 12 are lost, the acquirer may initiate a reversal.

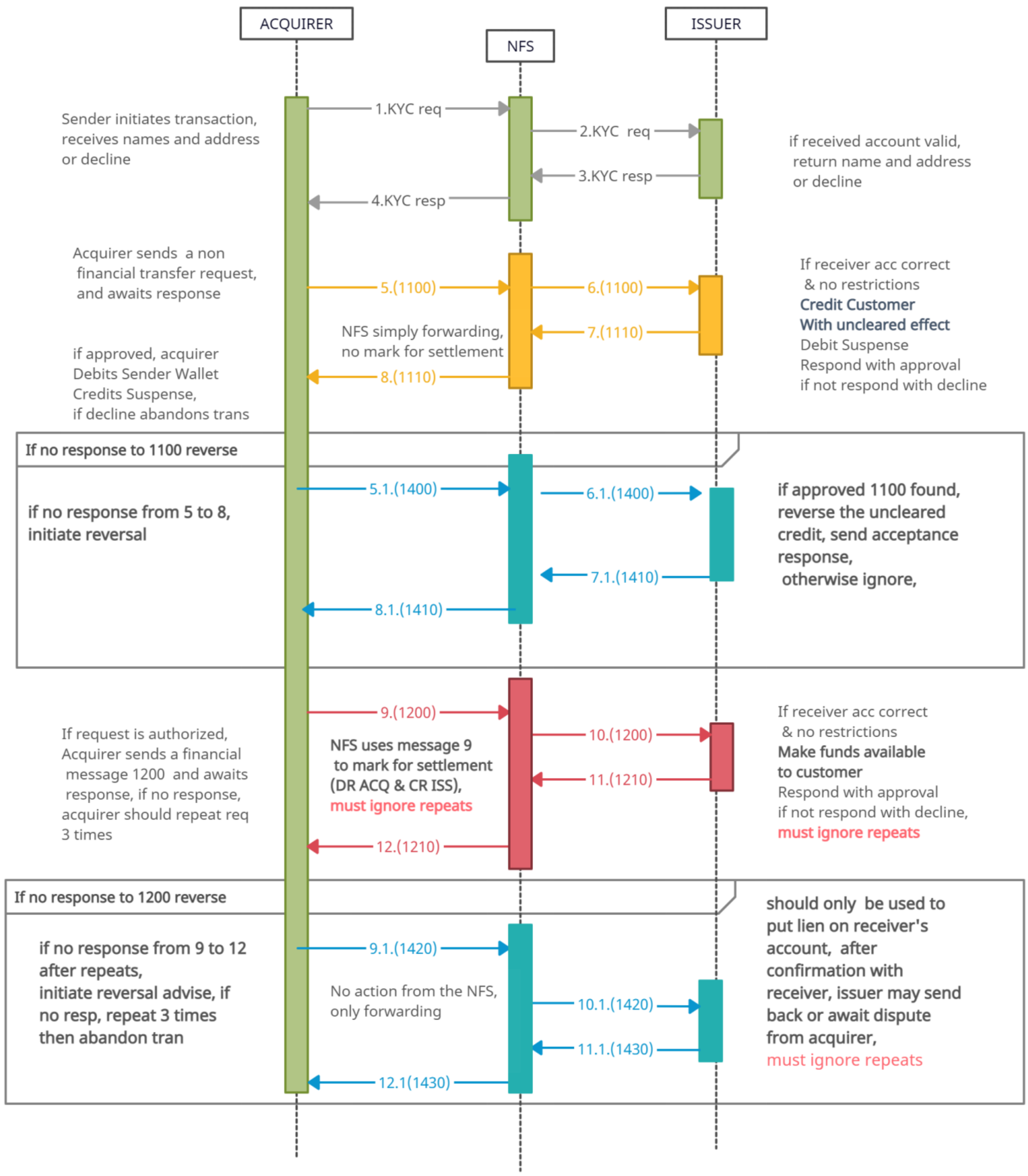

Figure 10. Proposed integration model

4.6.2. Message Failure Scenarios

Failure at KYC level: Failure at any of messages 1 to 4 will result in acquirer timing out and restarting the transaction.

Failure 1100 level: For failures at messages 5 or 6, the acquirer will time out and send a reversal 1400. Because no prior 1100 would be found, the issuer would ignore this reversal and there would not be any impact on any participant. The NFS simply forward the message in this case.

Failure 1100 level messages: For failures at 7 or 8, the acquirer times out and send a reversal. In this case the issuer reverses the credit with un-cleared effect which was earlier passed to the receiver. The funds would always be available because the receiver did not have access to them. The NFS simply forward the message even in this case as in figure 11.

Failure at 1200 level: After sending a 1200 and there is no response, the acquirer repeats the 1200 three (3) times after each timeout. The NFS and issuer must retransmit responses any prior 1200 was received. If there is no response after the third attempt, the acquirer may initiate a non-financial reversal advice 1420. The reason acquirer cannot send a financial impact reversal, is to protect the receiver from dishonest senders who would initiate a reversal after a successful transaction. The 1420 reversal advice may be used by the issuer to put a lien on the recipient's account pending intervention. The specific actions are depicted in figures 11, 12 and 13 and described in next paragraphs.

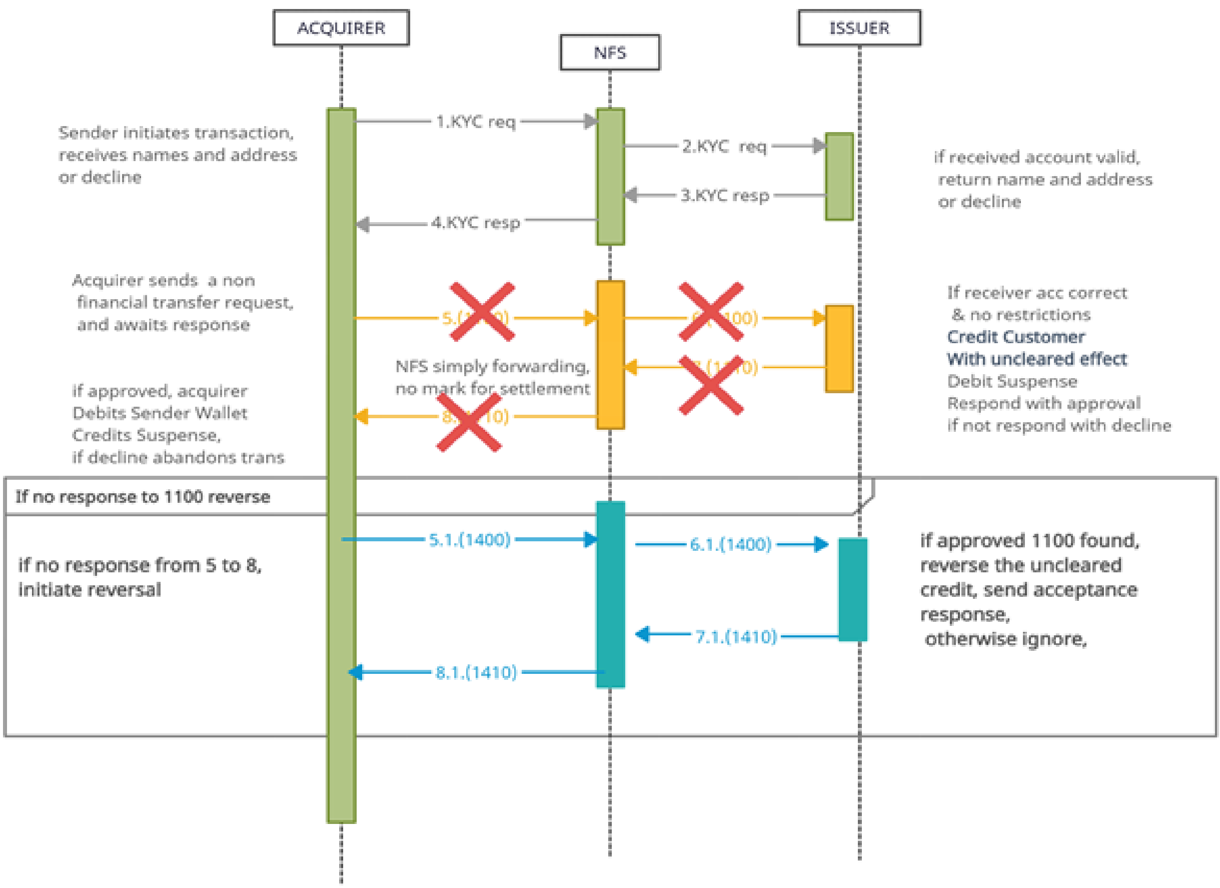

Figure 11. Failure at messages 5 or 6

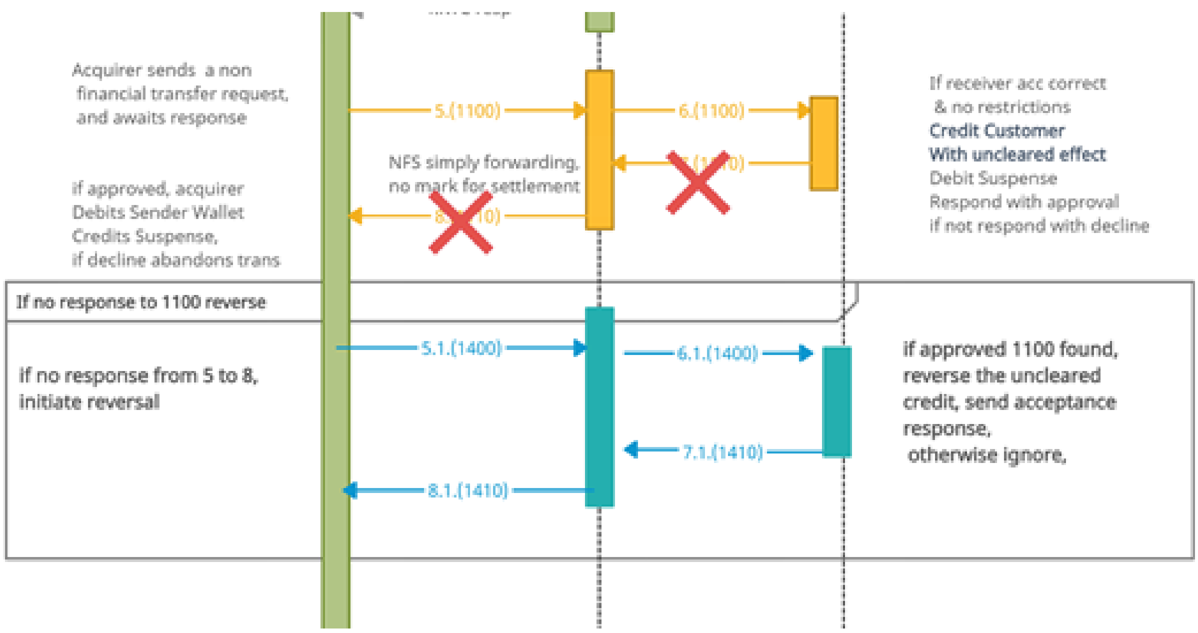

Figure 12. Failure at messages 7 and 8

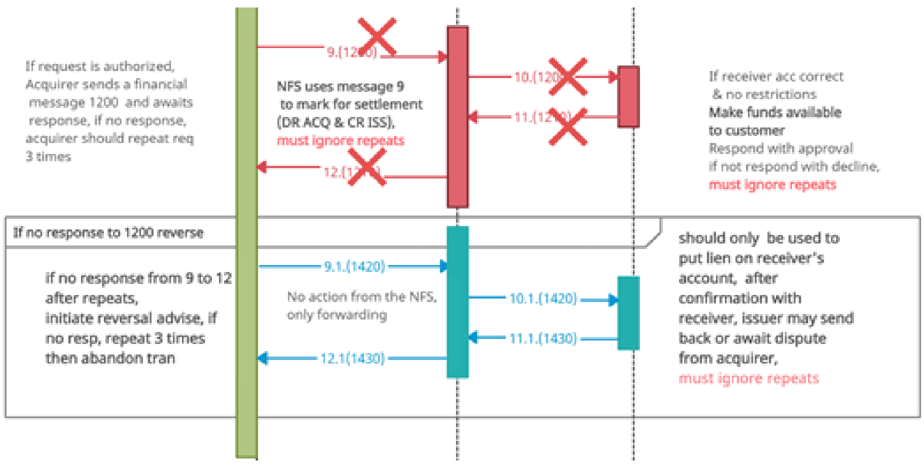

Figure 13. Failure at messages 9 to 12

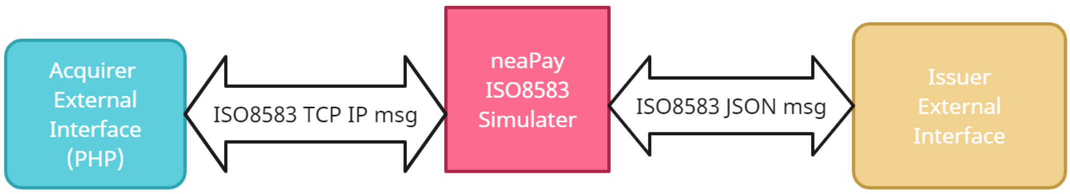

Figure 14. Prototype Architecture

Failure at 9: For a failure at message 9 even after repeats, there would be no settlement to the acquirer. The acquirer would eventually be in excess position as they would have already debited the sender's wallet while the issuer would be at a net position of 0 as the credit to the receiver's account would have not cleared. After receiving clearing files the next day, the acquirer would know that their request had not reached the NFS and would then automatically reverse the funds to the sender's wallet. Similarly, after receiving files the next day, the issuer would know that there was no financial 1200 message sent for the 1100 and would reverse the un-cleared credit on receiver's account to their suspense account; any 1420 messages would have also been ignored because no prior 1200 would have been received. The sender may simply initiate a new transaction in this case.

Failure at 10: For failure at message 10 even after repeats, the NFS would debit the acquirer and credit the issuer, but the issuer would have not received the 1200 message to clear the un-cleared credit on the receiver's account. The issuer would have ignored any 1420 message because no prior 1200 would have been received nonetheless; the 1420 would not be needed as the receiver's account would already have a credit with un-cleared effect. This transaction would need intervention to confirm if the issuer should proceed to credit the recipient or reverse the transaction depending on the use case and the status of the transaction between the sender and the issuer. The transaction may follow the same pattern of dispute resolution as is currently happening for POS and ATM transactions where the sender of money initiates a dispute through their institution(acquirer in this case) or the proactive issuer in consultation with the receiver sends back these funds.

Failure at 11 or 12: For failures at either message 11 or 12 two scenarios may arise, one being that a 1420 was successfully received by the issuer and the other being no 1420 was received by the issuer. For both scenarios, the NFS would have debited the acquirer and credited the issuer, and the issuer would have cleared the credit to receiver's account making it available to use using 1200. However, if the 1420 was received by the issuer, a lien would be put on the account, if not then the customer would have access to the funds. If the transaction between sender and receiver was deemed successful by the two, then the issuer removes the lien in consultation with the acquirer. However, if the sender and acquirer deemed the transaction not successful and either abandoned it or performed a second successful transaction, then the acquirer in consultation with issuer may process a dispute same way it happens for POS and ATM transaction.

4.6.3. Data Field Customization

Data Fields and Data fields Population: out of the 168 ISO 8583 data fields, 25 were identified to be sufficient to meet the consumer payments use cases. These fields where redefined, and rules placed for population in requests and responses of the messages. Additionally, four types of message request/response pairs were identified as necessary. These Message Type Indicators (MTI) of these messages were **1100/1110-KYC, 1100/1110-payment request, 1200/1210-settlement, 1400/1410-reversal request** and **1420/1430-reversal advice**. The identified and customised data fields were as follows (comma separated) **F1,F2,F3,F4, F5,F7,F10,F11,F12,F15,F18,F32,F37,F38,F39,F43,F44,F 49,F50,F65,F90,F100,F102,F103 and F123.**

Detailed contents of this customization are found in annexure 1. The annexure shows redefinition of each of the 25 identified fields and the routing and field population rules per message type.

4.6.4. Testing and Validation

Testing and validation of the model involved development of a prototype model as per architecture in figure 14. To mimic the real world scenario, neaPay ISO8583 simulator from neaPay payment solutions was used to represent the switch at the NFS. To mimic an acquirer and issuer, two prototype interfaces were developed in PHP. The acquirer populated fields in an HTML form as per defined population rules, while the neaPay simulator and issuer interface would be configured to respond to messages as per message flow and data field population rules in Annexure I. The results and explanations of the simulations are contained in annexure II. The source code of the PHP interfaces is added in annexure III. The source code is able to run on any Wamp server supporting PHP 7.

It is worth noting that due to the whole encompassing nature of the research, only critical technical aspects of the model, as explained in foregoing section and in Annexure II, were simulated. There was no need to define specific customer or merchant interface apps of the acquirers and issuers as these would be inconsequential to the study, as long as these players were able to pack and unpack messages to and fro the NFS switch, based on the defined rules. There was also limitation on the settlement tracking capabilities of the neaPay ISO 8583simulator. Nonetheless, settlement capabilities are mere configurable on the real world switch at the NFS. These configurations are based on the definition of message floes and data field population.

The tests results demonstrated that it was feasible to implement the developed model based on the customized specifications of ISO 8583 in the integration model.

4.6.5. Clearing

The currently existing setup where participants access a designated SFTP site to receive their clearing files shall be maintained. The NFS shall generate and share clearing files with participants for each business day. The files shall contain summaries and detailed reports for each transaction that qualified for settlement. Additionally the detailed files shall also indicate any reimbursement fee or switching fee levied on a participant.

4.6.6. Settlements

Like in clearing, the NFS shall maintain the currently existing settlement setup where they send settlement instructions to BOZ to debit or credit a participant based on the net sum of a business day's transaction. The NFS should not combine several business day but send separate instruction for each day. This shall help with streamlined reconciliation by the participants. Non-Bank participants with no settlement account at BOZ shall find a sponsoring bank to stand in for their settlement obligations. To protect sponsors, the NFS should have a configurable that allows the sponsor to a daily debit limit tied to the sponsored members' collateral or other similar assets deposited with the sponsoring bank. This means as the NFS is processing 1200, cumulative successive 1200 per participant should be noted and if a participant reaches a certain limit, further 1200 from that participant would be declined.

4.6.7. Transaction Dispute Resolution and Reconciliation

The NFS should support dispute resolution through the Data Navigator system that is currently being used for ATM and POS. The NFS may facilitate revision and annexure to the existing dispute rules, dispute resolution guidelines for the non ATM and POS transactions. This is important as the transactions are push and not pull and hence liability shifts would have to be re aligned.

4.6.8. Participant on Boarding Procedure

The currently prescribed on boarding process by the NFS and BOZ shall be followed. Each member must apply to the Bank of Zambia for a Certificate of Designation before engaging the NFS. After meeting the requirements and successfully obtaining the certificate of designation from Bank of Zambia, the member shall then apply for membership on the NFS and would have to meet the prescribed requirements before they are on boarded.

4.6.9. Operational Aspects

Cost: The model resolves the N-squared integration problem in the ecosystem. This transcends into reduced management of all aspects of integration from the payment facilitating companies. This reduction in operational costs results in cheaper services offered to merchants and consumers further stimulating the use of cashless payments.

Profitability: reduction in costs implicitly translates into greater profit margins. While higher volumes introduced by more usage from reduced costs also results in higher reurns, further attracting more investments into digital payment solutions using the integration model.

Security: A central integration point allows for the regulator to easily control security standards of the ecosystem. The NFS is PCDISS and ISO 27001 security standards certified. Participants joining the ecosystem are also required to subscribe to such minimum security standards and continuous audits to ensure conformant to these standards. There are other related security standards that could be easily introduced such use of HSMS and latest encryption standards.

5. Conclusions

The study highlighted that ISO 8583 could be used to interconnect payment companies. This would be feasible as it would leverage on the existing infrastructure at Zambia Electronic Clearing house. The study showed that there was little integrations of payment companies in Zambia. This was attributed to lack of integration model that tackled issues around profitability, security, integration standards and regulation. The study demonstrated that an integration model would need to consider merchant and consumer sentiments towards digital payments. Merchants should be encouraged through to use digital payments as it comes with a lot of benefits for them. The study showed that customizing the ISO 8583 as per defined message flow and data element customization in this report would resolve most of the afore mentioned challenges and allow integration. Integration would result in the ultimate goal of having more transactions being cashless in Zambia.

ACKNOWLEDGEMENTS

Many challenges were faced in finishing this research; it is worth noting the persistent encouragement, support and patience from my supervisor Dr. Simon Tembo. I wish to also thank friends, family and colleagues who gave various support throughout the whole process.

Annexure I: Data Field Customization

Table 1 contains data field customization of the existing ISO 8583 interface specification at the Zambia Electronic Clearing House. The field customization concentrated only 25 necessary data fields to facilitate transfer the KYC, payment and transfer use cases, it excluded network specific data fields such as those used to encrypt for example the Acquirer Working Key (AWK) and the message header fields that detect the source of the message such as POS, ATM or E-Money. The actual implantation may include for fields as required by the NFS functionality.

Table 2. Data Field Customization

Field #	Type	Original Field	Customized Description	Customized Allowed Values
1	b 64	Bit map (b 128 if secondary is present and b 192 if tertiary is present)	to determine presence of data fields	bit map
2	n ..19	Primary account number (PAN)	The PAN is a series of digits used to identify a customer account or relationship. Depending on configuration this field may contain Virtual Primary Account Number (Virtual PAN). Virtual Primary Account number always will be present in ans..19 (LLVAR) format.	6 digit receiver institution ID + receiver's account. Meaning receivers account will have maximum 13 digits
3	n 6	Processing code	The processing code is a series of digits used to describe the effect of a transaction on the customer account and the accounts affected.	It shall be 31 KYC 02 TRANSFER AND 03 PAYMENT, Right most digits padded with 0s
4	n 12	Amount, transaction	The transaction amount gives the value of the funds requested by the cardholder in the local currency of the acquirer of the transaction. Usage of this field is dependent on context: The value in response messages (1210, 1410 and 1430) must match the value in the corresponding request or advice message (1200, 1400 and 1420).	fixed length left adjusted with 2 implied decimal places
5	n 12	Amount, settlement	Contains Transaction Amount (Field 4) converted to settlement currency as per rate in Field 10	same as F4 because F49 trxn currency and F50 settlement currency are all 967 implying f10 conversation rate is fixed 61000000=1
7	n 10	Transmission date & time	Contains the date and time the message was generated. It is set for each outgoing message and must be expressed in Co-ordinated Universal Time (UTC)	MMDDHHMMSS
10	n 8	Conversion rate, cardholder billing	The factor used in the conversion from transaction to cardholder (wallet)billing amount. The amount transaction is multiplied by the billing conversion rate to give the cardholder billing amount. The leftmost digit of this field signifies the number of decimal places in the rate, and the remaining 7 digits give the actual rate. For example: 69972522 represents 9.972522	shall be fixed 61000000=1.000000=1

Field #	Type	Original Field	Customized Description	Customized Allowed Values
11	n 6	Systems trace audit number	Contains a number assigned by the transaction acquirer to identify uniquely a transaction. The trace number remains unchanged for all messages within the life of the transaction.	6 digit numeric e.g. 123456 or123457
12	n 6	Time, local transaction	Date in format yymmdd)	(YYMMDD)
15	n 4	Date, settlement	to contain the date of the clearing files by the NFS. This shall only be included in responses to financial message 1200 and rev 1400(1210 & 1410) and should be populated by the NFS	MMDD
18	n 4	Merchant type	Merchant Category Code of Sender is expected to be assigned depending on the wallet type.	7777 for wallet/non merchant account or the currently used MCC for POS for merchants
32	n ..11	Acquiring institution identification code	Sender institutional ID	6 digit ZECHL assigned ID left adjusted and padded with 0s to the right.e.g. id000006=00000600000
37	an 12	Retrieval reference number	Contains a document reference supplied by the system retaining the original source information and used to assist in locating that information or a copy thereof.	concatenation of the transmission date (in Julian date format – "yddd"), hour (hh)derived from Field 7 . and STAN from f11
38	an 6	Authorization identification response	6 digit alpha numeric Code assigned by the receiver institution indicating approval. Not populated in 1100 but should be in 1110 and subsequent 1200/1210, 1400/1410 and 1420/1430	length 6 alpha numeric
39	an 2	Response code	A code which defines the action taken or to be taken as well as the reason for taking this action.	00 for approval and appropriate ISO decline for declines e.g 14 account not found
43	ans 40	Card acceptor name/location	Sender details name and location	description of sender province or district may be sufficient for address. Left adjusted pad with space to the right
44	an ..25	Reserved for national use	Merchant Category Code of Receiver is expected to be assigned depending on the wallet type.	7777 for wallet/non merchant account or the currently used MCC for POS for merchants
49	an 3	Currency code, transaction	967 for Zambian Kwacha ZMW	967
50	an 3	Currency code, settlement	967 for Zambian Kwacha ZMW	967
65	b 64	*Bit indicator of tertiary bitmap only*, tertiary bitmap data follows secondary in message stream.	secondary bit indicator	0 if not present and 1 if present
90	an 42	Original Data Elements	Concatenation of RRN,SENDER Institution ID, sender account, receiver institutional ID and receiver account numbers	F37 Rrn=12 digits F102 sender= 13max, F103 Receiver Acc= 13Max, Left adjusted pad with 0 to make 42
100	n ..11	Receiving institution identification code	Zechl assigned institution code of receiver same as first 6 in pan	6 digit padded with zeros to the right
102	ans ..28	Account identification 1	Sender wallet account	max 13 for uniformity purpose
103	ans ..28	Account identification 2	receiver wallet account	max 13 for uniformity purpose
123	ans ...999	Transaction description	Narration describing purpose of transaction or transfer. This is optional field in NON KCY 1100	Name and address in KYC 1100(ISSUER) Trans Details in the rest(ACQUIRER)

Table 3. Routing and Data Field Population per Message Type

Routing

On the NFS network, each participant is assigned a six digit institutional ID. When effecting a payment or transfer, the NFS shall use the Field 100 Receiving Institution ID to route the incoming message to the correct participant, and Field 11 Acquirer Institution ID to return the response. These fields shall be mandatory for all messages 1100/1110, 1200/1210, 1400/1410 and 1420/1430.

Population of Data Fields

KYC 1100/1110

At KYC level, message shall be a 1100/1110 pair with processing code '**310000'** and amount data fields shall be populated with zeros'000000000000'. If field 103 receiver's account is valid, the issuer shall respond with response code '00' in field 39 and the details of the KYC in field 123. If the latter account is invalid, the issuer shall decline putting an appropriate response code in field 39.

1100-KYC

For a KYC 1100 authorization request, the acquirer shall populate as follows

Field F2 pan: issuer 6 digit institutional ID + receiver's account of maximum length 13

Field F3 processing code: '310000'

Field F4 amount transaction: '000000000000'.

Field F5 amount settlement: '000000000000'.

Field F7 Transmission date & time: UTC date time in format (MMDDhhmmss),

Field F10 Conversion rate: '61000000',

Field 11 System Trace Audit Number: 6 digit transaction sequence(incremented for each transaction),

Field 12 Local time: local time in format (YYMMDD),

Field 15 Date Settlement: format (MMDD), not included as it will be populated by ZECHL for 1200s only

Field 18, Merch Type: four digit wallet type sender 7777 for wallet/non merchant account or the currently used MCC for POS for merchants,

Field 32 Acquiring institution identification code: 6 digits ZECHL assigned institution ID padded with Zeros to the right,

Field 37 Retrieval reference number: concatenation of the transmission date (in Julian date format – "YDDD") derived from F12, hour (HH) derived from Field 7 and STAN from f11,

Field 38 Authorization identification response: not included as it is expected in response only,

Field 39 Response code: not included as it is expected in response only,

Field 43 Card acceptor name/location: Sender's name and or location (location may be town or district) this is a left adjusted fixed length field (must be 40) hence may be padded with which space to the right,

Field 44 Receiver Merchant Type: not populated, to be populated by issuer when sending back KYC data

Field 49 Currency code, transaction: 967

Field 50 Currency code, settlement: 967

Field 90 Original Data Elements: concatenation of RRN, SENDER ACC and RECEIVER ACC (F37, F102, F103) fixed length 42 left adjusted to be padded with zeros to the right

Field 100 Receiving institution identification code: 6 digits ZECHL assigned ID padded with zeros to the right,

Field 102 Account identification 1: Senders wallet account of maximum length 13,

Field 103 Account identification 2: Receivers wallet account of maximum length 13,

Field 123 Transaction description: NOT populated, to be used by the issuer when sending back KYC data

1110- KYC

For a KYC 1110 authorization response, shall echo all fields in the 1100 and add the following:-

Field 38 Authorization identification response: a six digit approval code if approved or blank if not approved,

Field 39 Response code: '00' If account exists' or '14' if account does not exist

Field 123 Transaction description: Receivers name and Address or 'Account Not Found'

Field 44 Receiver Merchant Type: if field 39 is '00', issuer must also respond with 7777 for wallet/non merchant account or the currently used MCC for POS for merchants

Messages for Payment, Transfer and Cash-in use case

If KYC message was approved, the acquirer generates a new 1100 message as per defined message flow and populates as following

1100 request

For an 1100 authorization request, the acquirer shall populate as follows

Field F2 pan: issuer 6 digit institutional ID + receiver's account of maximum length 19,

Field F3 processing code: '020000' for transfers or '030000' for payments.

Field F4 amount transaction: the transactional amount with 2 implied decimal places,

Field F4 amount settlement: the transactional amount with 2 implied decimal places,

Field F7 Transmission date & time: UTC date time in format (MMDDhhmmss),

Field F10 Conversion rate: '61000000',

Field 11 System Trace Audit Number: a new 6 digit transaction sequence(incremented for each transaction), Field 12 Local time: local time in format (YYMMDD),

Field 15 Date Settlement: format (MMDD), not included as it will be populated by ZECHL for 1200s only

Field 18, Merch Type: four digit wallet type sender 7777 for wallet/non merchant account or the currently used MCC for POS for merchants,

Field 32 Acquiring institution identification code: 6 digit ZECHL assigned institution ID padded with Zeros to the right,

Field 37 Retrieval reference number: concatenation of the transmission date (in Julian date format – "YDDD") derived from F12, hour (HH) derived from Field 7. and STAN from f11,

Field 32 Acquiring institution identification code: 6 digit ZECHL assigned institution ID padded with Zeros to the right,

Field 37 Retrieval reference number: concatenation of the transmission date (in Julian date format – "YDDD") derived from F12, hour (HH) derived from Field 7. and STAN from f11,

Field 38 Authorization identification response: not included as it is expected in response only,

Field 39 Response code: not included as it is expected in response only,

Field 43 Card acceptor name/location: Sender's name and or location (location may be town or district) this is a left adjusted fixed length field (must be 40) hence may be padded with which space to the right,

Field 44 Receiver Merchant Type: not populated, to be populated by issuer in 1110 response

Field 49 Currency code, transaction: 967

Field 50 Currency code, settlement: 967

Field 90 Original Data Elements: concatenation of RRN, SENDER ACC and RECEIVER ACC (F37, F102, F103) fixed length 42 left adjusted to be padded with zeros to the right,

Field 100 Receiving institution identification code: 6 digits ZECHL assigned ID padded with zeros to the right,

Field 102 Account identification 1: Senders wallet account of maximum length 13,

Field 103 Account identification 2: Receivers wallet account of maximum length 13,

Field 123 Transaction description: Senders Narration ANS character max 100(optional),

1110 response

For an 1110 authorization response, the issuer echoes the populated fields in the 1100 request and add field 38 and 39 and 44 as below

Field 38 Authorization identification response: a six digit approval code if approved or blank if not approved,

Field 39 Response code: '00' for approval or appropriate decline code as per ISO 8583 for declines,

Field 44 Receiver Merchant Type: if field 39 is '00', issuer must also respond with 7777 for wallet/non merchant account or the currently used MCC for POS for merchants

1200 From Acquirer to NFS

For a financial 1200, the acquirer shall maintain the fields as returned in the approved 1110 from the issuer.

1200 from NFS to ISSUER

At this stage the NFS is expected to mark the transaction for settlement and hence shall mark and add:-

Field 15 Date Settlement: format (MMDD), the date of the clearing files which for most transactions will be date +1 expect those transactions around cut-off times, which may have transaction date and settlement date being the same.

1210 from Issuer all the way back to Acquirer

The issuer shall check if they had received a prior 1100 using combination of RRN, sender institution ID and approval code. If there is a prior message, the issuer accepts the transaction and returns the message as received. If the issuer cannot look up prior 1100, it declines with appropriate response code overwriting **Field 39 Response code:**

1400/1420

This is shall only be used by the acquirer in 1100 time outs and declines at 1210 level. The acquirer shall maintain the fields as received in the 1110 message and only populate:-

Field 90 Original Data Elements: concatenation of RRN, SENDER ACC and RECEIVER ACC (F37, F102, F103) fixed length 42 left adjusted to be padded with zeros to the right as contained in the message being reversed Code in 1100/1110 for 1400 or 1200/1210 for 1420

Field 11 System Trace Audit Number: 6 digit transaction sequence(incremented for each transaction). A reversal should have its own STAN but retain the original date time

The NFS shall only forward the 1400 or1420, however, the issuer shall use the 1400 to unblock funds but only use the 1420 to put lien on receivers account awaiting intervention in liaison with the receiver and the acquirer.

Annexure II: Testing and Validation

Table 4. Testing and validation results

neaPay Simulator

The simulator was able to receive ISO 8583 message from acquirer, forward to the issuer and return the appropriate response

External Interface acquirer;

The external interface was developed using PHP, whose functionality was to be able to pack an ISO 8583 message as described in the message flow and data field section. The interface could act as acquirer or issuer. For streamlined testing and demonstration, the interface acted as acquirer, the simulator received, unpacked and packed the ISO 8583 as JSON and was sent to a PHP script to respond to the incoming messages. Below we discuss the acquirer interface and code.

External Interface (ISO 8583.PHP & ISO8583.HTML)

ISO 8583.PHP

Data Field Classes

Before identification and customization of needed data fields to meet the use cases, each of the 128 ISO 8583 data fields were implemented by a PHP class with two properties, bit and value. By default, the bit is set to 0 and the value is not assigned, when the value is set, the bit is set to 1. A field class has two methods, a set method and a read method. The set method takes the value of the field as the attribute and assigns this value and sets the bit to 1. The read method simply returns the value of the field. The functions are defined based on the specification of the data field. A data field may be of fixed length or variable length. Variable length fields require that leading digits specify the length. Figure 1 shows the code snippet for one of the PHP class objects implementing a Filed 02 data element.

```
<?php//each filed definec as a class with properties $bit and value and  set and get methos
class F02{
    public $bit=0;  public $value;
    public function set_value($value){
        $this->value =str_pad(strlen($value), 2, '0', STR_PAD_LEFT). $value;    $this->bit=1;
        }
    public  function read_values(array $array,$offset){
        $field_length=null; $leading_digits=2;
        if($leading_digits==0){$length=19;}
        if($leading_digits==1){$length=$array[$offset];}
        if($leading_digits==2){$length=$array[$offset].$array[$offset+1];}
        if($leading_digits==3){$length=$array[$offset].$array[$offset+1].$array[$offset+2];}
        $offset =$offset+$leading_digits;   $values=array();
        for($i=$offset;$i<$offset + $length;$i++){$values[]=$array[$i];}
        $this->value=implode("",$values);
        echo "<br/><b/>F02:".$this->value; return $offset=$offset+$length; }
        }
```

Figure 1

Build Message Function

Global function build_message(MTI,F01,F02,…,F128) takes in an MTI and instances of all of the 128 data fields as parameters. The fields are pushed into a holding array from which a bitmap is made by concatenating the bitmaps of the data fields in the array. The value of each data is also extracted. The MTI, bitmap and data fields are put together to form an ISO 8583. The message length is appended to the front of the message and the message is packed as ASCII. Function build_message(…) returns a message to send to the neaPay ISO 8583 simulator. Figure 2 shows PHP code snippet to of this function.

```
    for ($x =1 ; $x <strlen($bitmap); $x++) {
        //echo $fields[$x]->value."no".$x;
        //if($fields[$x]->value==null){}
        if($fields[$x]->value !==null){  $message .=$fields[$x]->value; } //add only those fields present
    } // end for
    //echo  $message;
    //inplace of base convert break btmap into four bit array and use base convert for each 4 groupings , this
    $tmp=str_split($bitmap,4);
    $l=0;
    $bit="";
    while($l<count($tmp)){
        $bit .=base_convert($tmp[$l],2,16); $l++;
        }

    $bitmapTemp=str_split($bit,2);//split into two charactor array so they may be sent as charactors

    for ($y=0;$y<count($bitmapTemp);$y++){
        $bitmap_hex .=chr(base_convert($bitmapTemp[$y],16,10));//encoding as asscii
    }
    //echo strlen($bitmap_hex);echo $bitmap_hex;


    $message_length=strlen($mti.$bitmap_hex.$bitmap_hex.$message);//bit map has to be twice because it is in he
    $lengtharray=str_split(str_pad(base_convert($message_length,10,16), 4, '0', STR_PAD_LEFT),2);//first conver
    $message_length_in_hex= chr(base_convert($lengtharray[0],16,10)).chr(base_convert($lengtharray[1],16,10));

    $final_message = $message_length_in_hex.$mti.$bitmap_hex.$message;

    //writing to file for now, to be written to database later

    //echo "hex bitmap".$bitmap_hex;echo " binary bitmap".$bitmap;
    return $final_message; //*/
    //return "end";
} // END BUILD MESSAGE FUNCTION
```

Figure 2

Send Message function

There is a function send message (message) whose purpose is to send the message to the neaPay simulator and listen for, and handle replies. Figure 3 shows snippet of the code. Localhost address is used as the neaPay simulator is running on local machine on port 9009.

```
function  send_message($message){
    $host    = "127.0.0.1";
    $port    = 9009;
    $socket = socket_create(AF_INET, SOCK_STREAM, 0) or die("Could not create socket\n");
// connect to server
    $result = socket_connect($socket, $host, $port) or die("Could not connect to server\n");
    // send string to server
    socket_write($socket, $message, strlen($message)) or die("Could not send data to server\n");
    $result = socket_read ($socket, 1024) or die("Could not read server response\n");
// convert the returned message into array for easy manipulation
    socket_close($socket);


    //incoming message put in array for easy manipulation
    $array =str_split($result,1);
    $offset=null;//used to loop through incoming message


    //////////////////////////////////////////////////////////////////////////////////////////
    //echo bin2hex($array[8]);
    $incoming_bitmap="";//to hold incoming bitmap
    $incoming_bitmap_len=null;//length of bit map  8 for 64 and 16 for 128

    //if fisrt bit is 0 then there is no secondary bit and hence  8 charactors which in actual sense repres
    if(substr(str_pad(base_convert(bin2hex($array[6]).bin2hex($array[7]),16,2), 16, '0', STR_PAD_LEFT),0,1)

    // get the bitmap in binary and put it in array for maipulation
    for($i=6;$i<6+$incoming_bitmap_len;$i++){$incoming_bitmap .=str_pad(base_convert(bin2hex($array[$i].$ar

    $bits= str_split($incoming_bitmap,1);
```

Figure 3

Transact function

Finally there is function transact() which simpley creates instances of the 128 data fields, receives form data via POST from a portal script iso8583.html. the function checks which of the 128 datafields have form data aswell and the MTI set. The POST message also has the ISO 8583 simulator IP address and port number. The function uses the created instances and form data to call the buld_message and send_message functions to buld and send the message respectively. Figure 4 is snippet code of the transact function

```php
<?php
function transaction(){
    $f1=new F01(); $f2=new F02(); $f3=new F03(); $f4=new F04(); $f5=new F05(); $f6=new F06(); $f7=new F07(); $f8=new F08(); $f9=new F09(); $f10=new F1C

//$outgoing_fields=array();
//if($_POST["F02"]!==""){ $f2->set_value($_POST["F02"]);echo "F02: Entered:\t".$_POST["F02"]."\tFinal including length:\t".$f2->value."<br>";}
$mti=$_POST["mti"];
echo "MTI:\t".$mti."<BR>";
if($_POST["F02"]!==""){ $f2->set_value($_POST["F02"]);echo "F02: Entered:\t".$_POST["F02"]."\tFinal including length:\t".$f2->value."<br>";}
if($_POST["F03"]!==""){ $f3->set_value($_POST["F03"]);echo "F03: Entered:\t".$_POST["F03"]."\tFinal including length:\t".$f3->value."<br>";}
if($_POST["F04"]!==""){ $f4->set_value($_POST["F04"]);echo "F04: Entered:\t".$_POST["F04"]."\tFinal including length:\t".$f4->value."<br>";}
if($_POST["F05"]!==""){ $f5->set_value($_POST["F05"]);echo "F05: Entered:\t".$_POST["F05"]."\tFinal including length:\t".$f5->value."<br>";}
if($_POST["F06"]!==""){ $f6->set_value($_POST["F06"]);echo "F06: Entered:\t".$_POST["F06"]."\tFinal including length:\t".$f6->value."<br>";}
if($_POST["F07"]!==""){ $f7->set_value($_POST["F07"]);echo "F07: Entered:\t".$_POST["F07"]."\tFinal including length:\t".$f7->value."<br>";}
if($_POST["F08"]!==""){ $f8->set_value($_POST["F08"]);echo "F08: Entered:\t".$_POST["F08"]."\tFinal including length:\t".$f8->value."<br>";}
if($_POST["F09"]!==""){ $f9->set_value($_POST["F09"]);echo "F09: Entered:\t".$_POST["F09"]."\tFinal including length:\t".$f9->value."<br>";}
if($_POST["F10"]!==""){ $f10->set_value($_POST["F10"]);echo "F10: Entered:\t".$_POST["F10"]."\tFinal including length:\t".$f10->value."<br>";}
if($_POST["F11"]!==""){ $f11->set_value($_POST["F11"]);echo "F11: Entered:\t".$_POST["F11"]."\tFinal including length:\t".$f11->value."<br>";}
if($_POST["F12"]!==""){ $f12->set_value($_POST["F12"]);echo "F12: Entered:\t".$_POST["F12"]."\tFinal including length:\t".$f12->value."<br>";}
if($_POST["F13"]!==""){ $f13->set_value($_POST["F13"]);echo "F13: Entered:\t".$_POST["F13"]."\tFinal including length:\t".$f13->value."<br>";}
if($_POST["F14"]!==""){ $f14->set_value($_POST["F14"]);echo "F14: Entered:\t".$_POST["F14"]."\tFinal including length:\t".$f14->value."<br>";}
if($_POST["F15"]!==""){ $f15->set_value($_POST["F15"]);echo "F15: Entered:\t".$_POST["F15"]."\tFinal including length:\t".$f15->value."<br>";}
if($_POST["F16"]!==""){ $f16->set_value($_POST["F16"]);echo "F16: Entered:\t".$_POST["F16"]."\tFinal including length:\t".$f16->value."<br>";}
if($_POST["F17"]!==""){ $f17->set_value($_POST["F17"]);echo "F17: Entered:\t".$_POST["F17"]."\tFinal including length:\t".$f17->value."<br>";}
if($_POST["F18"]!==""){ $f18->set_value($_POST["F18"]);echo "F18: Entered:\t".$_POST["F18"]."\tFinal including length:\t".$f18->value."<br>";}
if($_POST["F19"]!==""){ $f19->set_value($_POST["F19"]);echo "F19: Entered:\t".$_POST["F19"]."\tFinal including length:\t".$f19->value."<br>";}
....
....

$message =build_message($mti,$f1, $f2, $f3, $f4, $f5, $f6, $f7, $f8, $f9, $f10, $f11, $f12, $f13, $f14, $f15, $f16, $f17, $f18, $f19, $f20, $f21, $f22,
send_message($message);
}
```

Figure 4. PHP transaction function definition code snippet

ISO8583.HTML

Figure 5 shows snippet of the script holding form data of the data fields.

```html
<!DOCTYPE html>
<html>
<head>

</head>
<body>

<h1>INTEGRATION OF DIGITAL PAYMENT SCHEMES USING ISO 8583</h1>
<h3>Create a Message and Submit</h3>


<form action="ISO8583.php" method="post">
Host:<input type="text" name="host" value ="127.0.0.1">Port:<input type="text
<br>F01:<input type="text" name="F01">
F02:<input type="text" name="F02">
F03:<input type="text" name="F03">
F04:<input type="text" name="F04">
F05:<input type="text" name="F05"><br>
F06:<input type="text" name="F06">
F07:<input type="text" name="F07">
F08:<input type="text" name="F08">
F09:<input type="text" name="F09">
F10:<input type="text" name="F10"><br>
F11:<input type="text" name="F11">
F12:<input type="text" name="F12">
F13:<input type="text" name="F13">
F14:<input type="text" name="F14">
F15:<input type="text" name="F15"><br>
F16:<input type="text" name="F16">
F17:<input type="text" name="F17">
F18:<input type="text" name="F18">
F19:<input type="text" name="F19">
F20:<input type="text" name="F20"><br>
F21:<input type="text" name="F21">
F22:<input type="text" name="F22">
```

Figure 5. HTML form configured to send POST data to external interface

Figure 6 shows sample of the displayed data fields for the user.

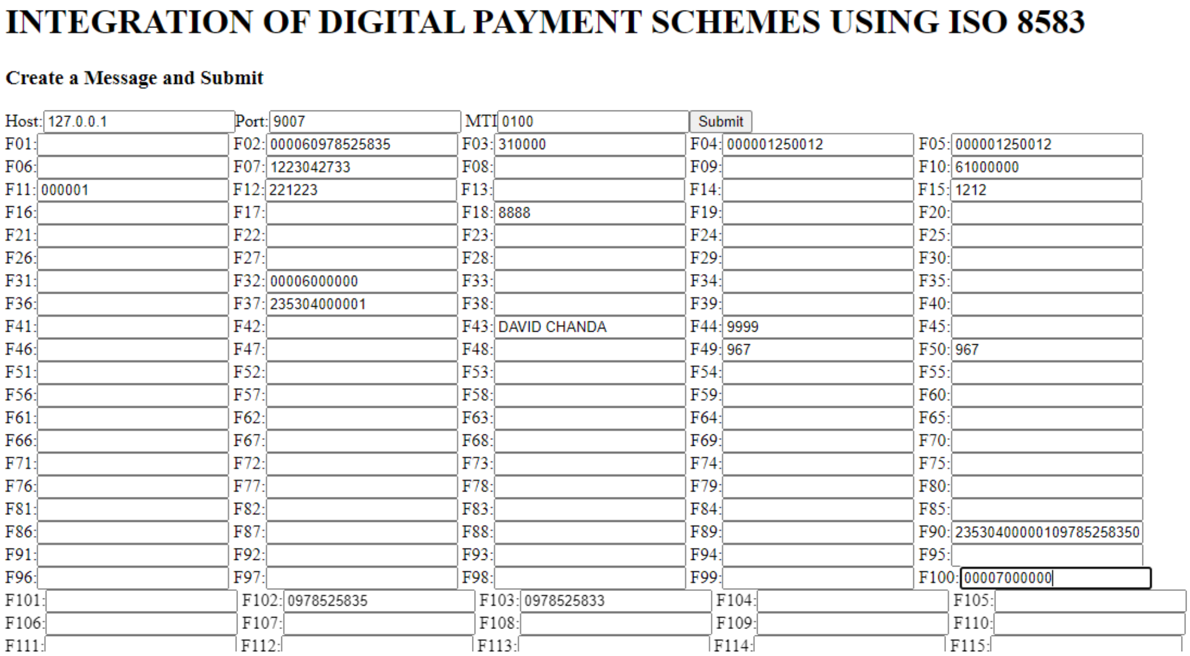

Figure 6

ISSUER SCRIPT (SERVER.PHP)

Figure 7 shows the implantation of the issuer interface that receives JSON ISO 8583 message from the neaPay simulator. The issuer logic checks for MTI and processing code value to approve or decline a transaction. When approving, the issuer adds approval code, response code and any relevant field as per use case. For example, if the MTI is 1100 (auth request) and processing code is '310000' (KYC request), the issuer returns KYC data in field 123 if transaction is approved.

```
<?php
$data = json_decode(file_get_contents('php://input'), true);

$myfile = fopen("output.txt", "w") or die("Unable to open file!");
$account="0978525835";$name="David Chanda"; $address ="lusaka";
$kyc="310000";  $mcc= "7777";
if($data[3]["value"]==$kyc){
	//71 is index of receiver account in json
	if($data[71]["value"]==$account){
		$data[35]["value"]="apprvd";
	$data[36]["value"]="00";  //approve
	$data[72]["value"]=$name.$address;//KYC DETAILS
	$data[41]["value"]=$mcc;//wallet
	}else{
		$data[35]["value"]="      ";//DECLINED APPROVAL ASSIGED BLANK
		$data[36]["value"]="14";  //decline 14 is invalid account
	}
}else{
if($data[71]["value"]==$account){
	//hold funds and respond with approval
	$data[35]["value"]="apprvd";
	$data[36]["value"]="00";  //approve
	$data[41]["value"]=$mcc;//wallet
	}else{
		//else decline
		$data[35]["value"]="      ";//DECLINED APPROVAL ASSIGED BLANK
		$data[36]["value"]="14";  //decline 14 is invalid account
	}
	}
fwrite($myfile,http_build_query($data,'','| ') );
fclose($myfile);
$payload = json_encode($data);
header('Content-type: application/json');
echo $payload ;
//echo "hello123";
//-------------------------------------------------
?>
```

Figure 7. Issuer interface code snippet issuer interface code snippet

SIMULATION TESTS

KYC MESSAGE- EXISTING ACCOUNT

Figure 4-28 shows necessary data for a KYC message filled in the acquirer interface form. To allow the issuer identify this message as KYC request, the processing code in field 3 was populated with '310000' while fields such as approval code, response code and f123 were not populated as these are what the issuer would need to populated depending on whether the receiver account in field 103 is valid or not. Figure 4-29 shows the response received after the message was sent to the neaPay system which in turn forwarded to the issuer script. The figure shows that the receiver's account existed and hence the issuer populated field 39 with 00 and put the receiver's name and location in field 123 as per customized specification. Figures 8,9 and 10 show that the message from the acquirer had reached the neaPay simulator which in turn forwarded to the issuer, the issuer responded back to the neaPay simulator.

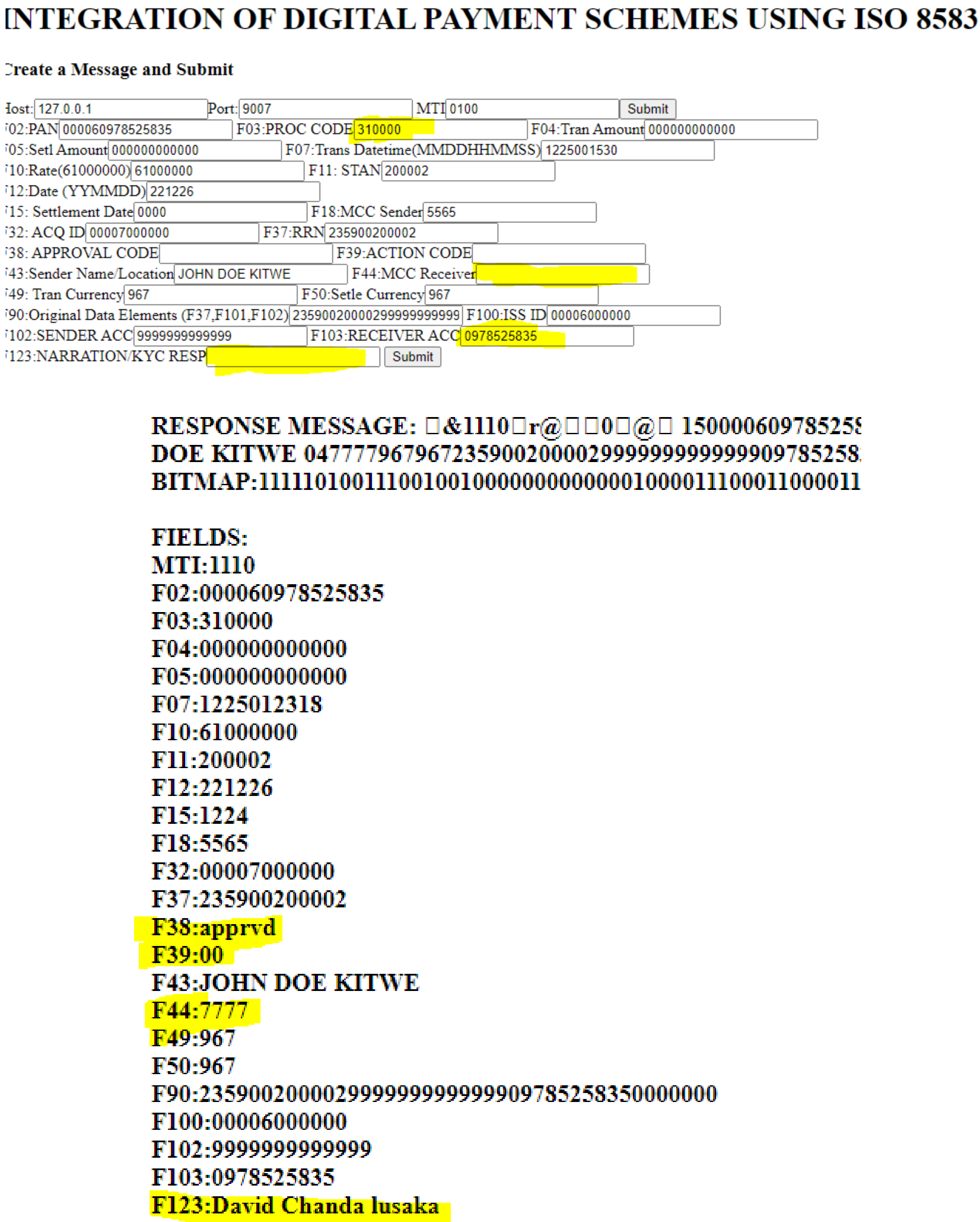

Figure 8. Message response received by the external interface

```
25-12-22 01:23:18:677:- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
25-12-22 01:23:18:677:CNV: Message received by Converter
25-12-22 01:23:18:677:CNV: MessageType                   :0100
25-12-22 01:23:18:677:CNV: Bitmap                        :FA7240010E30C00000000004016000020 bits:1111101001110010010
25-12-22 01:23:18:677:CNV: F02_PAN                       :000060978525835
25-12-22 01:23:18:679:CNV: F03_ProcessingCode            :310000
25-12-22 01:23:18:680:CNV: F04_AmountTransaction         :000000000000
25-12-22 01:23:18:680:CNV: F05_AmountReconciliation      :000000000000
25-12-22 01:23:18:680:CNV: F07_TransmissionDateTime      :1225001530
25-12-22 01:23:18:680:CNV: F10_ConvRateBill              :61000000
25-12-22 01:23:18:680:CNV: F11_SystemTraceAuditNumber    :200002
25-12-22 01:23:18:680:CNV: F12_DateTimeLocalTransaction  :221226
25-12-22 01:23:18:680:CNV: F15_DateSettlement            :0000
25-12-22 01:23:18:680:CNV: F18_MerchantType              :5565
25-12-22 01:23:18:681:CNV: F32_AcquiringInstitutionIdenti:00007000000
25-12-22 01:23:18:681:CNV: F37_RetrievalReferenceNumber  :235900200002
25-12-22 01:23:18:681:CNV: F38_ApprovalCode              :
25-12-22 01:23:18:681:CNV: F39_ActionCode                :
25-12-22 01:23:18:681:CNV: F43_CardAcceptorNameLocation  :JOHN DOE KITWE
25-12-22 01:23:18:681:CNV: F44_AdditionalResponseData    :
25-12-22 01:23:18:681:CNV: F49_CurrencyCodeTransaction   :967
25-12-22 01:23:18:681:CNV: F50_CurrencyCodeReconciliation:967
25-12-22 01:23:18:682:CNV: F90_OriginalDataElements      :2359002000029999999999999097852583500000000
25-12-22 01:23:18:682:CNV: F100_RecInstIdCode            :00006000000
25-12-22 01:23:18:682:CNV: F102_AccountId1               :9999999999999
25-12-22 01:23:18:682:CNV: F103_AccountId2               :0978525835
25-12-22 01:23:18:682:CNV: F123_Reserved                 :
25-12-22 01:23:18:682:- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
25-12-22 01:23:18:736:CNV: Match found in Issuer Cases: 01|NFS KYC Authorization Response|010%|0*|3*|*|*
25-12-22 01:23:18:756:CNV: Case found:01:NFS KYC Authorization Response
```

Figure 9. NeaPay console transaction log for KYC message sent

```
25-12-22 01:23:19:977:- - - - - - - - - - - - - - - - - - - - - - - - -
25-12-22 01:23:19:977:CNV: Message response sent  by Converter
25-12-22 01:23:19:977:CNV: MessageType                   :1110
25-12-22 01:23:19:977:CNV: Bitmap                        :FA7240010E30C00000000004016000020 bits:111110
25-12-22 01:23:19:979:CNV: F02_PAN                       :000060978525835
25-12-22 01:23:19:979:CNV: F03_ProcessingCode            :310000
25-12-22 01:23:19:979:CNV: F04_AmountTransaction         :000000000000
25-12-22 01:23:19:979:CNV: F05_AmountReconciliation      :000000000000
25-12-22 01:23:19:979:CNV: F07_TransmissionDateTime      :1225012318
25-12-22 01:23:19:979:CNV: F10_ConvRateBill              :61000000
25-12-22 01:23:19:979:CNV: F11_SystemTraceAuditNumber    :200002
25-12-22 01:23:19:979:CNV: F12_DateTimeLocalTransaction  :221226
25-12-22 01:23:19:980:CNV: F15_DateSettlement            :1224
25-12-22 01:23:19:980:CNV: F18_MerchantType              :5565
25-12-22 01:23:19:980:CNV: F32_AcquiringInstitutionIdenti:00007000000
25-12-22 01:23:19:980:CNV: F37_RetrievalReferenceNumber  :235900200002
25-12-22 01:23:19:980:CNV: F38_ApprovalCode              :apprvd
25-12-22 01:23:19:980:CNV: F39_ActionCode                :00
25-12-22 01:23:19:980:CNV: F43_CardAcceptorNameLocation  :JOHN DOE KITWE
25-12-22 01:23:19:980:CNV: F44_AdditionalResponseData    :7777
25-12-22 01:23:19:981:CNV: F49_CurrencyCodeTransaction   :967
25-12-22 01:23:19:981:CNV: F50_CurrencyCodeReconciliation:967
25-12-22 01:23:19:982:CNV: F90_OriginalDataElements      :2359002000029999999999999097852583500000000
25-12-22 01:23:19:983:CNV: F100_RecInstIdCode            :00006000000
25-12-22 01:23:19:983:CNV: F102_AccountId1               :9999999999999
25-12-22 01:23:19:983:CNV: F103_AccountId2               :0978525835
25-12-22 01:23:19:983:CNV: F123_Reserved                 :David Chanda lusaka
25-12-22 01:23:19:983:- - - - - - - - - - - - - - - - - - - - - - - - -
25-12-22 01:23:20:037:SYS:Set:MessageType:ascii:1110
25-12-22 01:23:20:038:SYS:Buffer added:31313130
25-12-22 01:23:20:038:SYS:Set:Bitmap:binary:FA7240010E30C00000000004016000020
25-12-22 01:23:20:038:SYS:Buffer added:FA7240010E30C00000000004016000020
25-12-22 01:23:20:038:SYS:bitmap found:FA7240010E30C00000000004016000020
```

Figure 10. neaPay console transaction log for KYC message response

NON EXISTANT ACCOUNT

The figures 11, 12 and 13 show the results when the receivers account in the KYC is invalid. The issuer responds with '14' in response code data field to notify the acquirer that the account could not be located. The issuer does not populate receiver details in field 123 nor the receiver's MCC in field 44

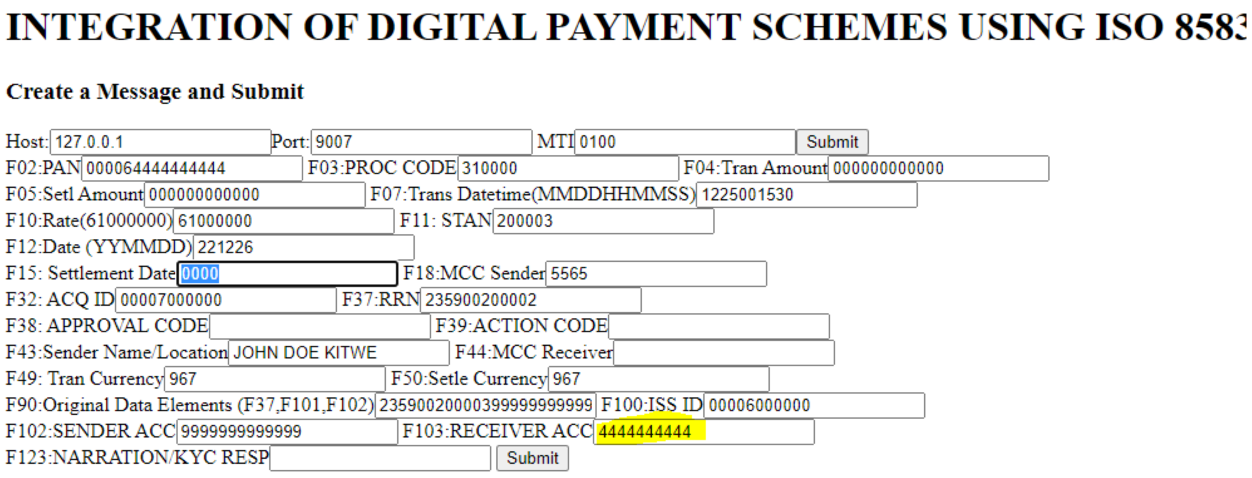

Figure 11. KYC request on invalid account sent to external acquirer interface

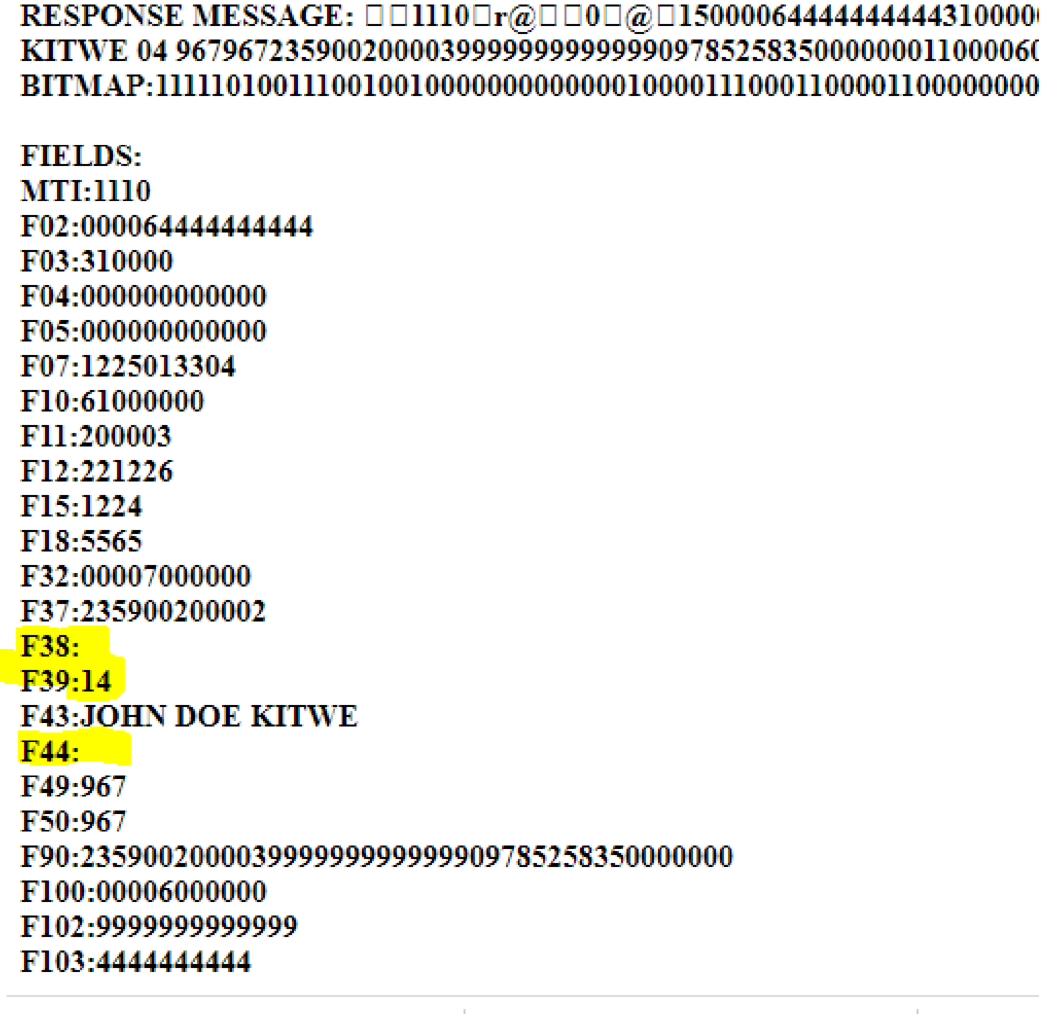

Figure 12. Declined response 14 invalid account

```
- -- -- --:-----------
5-12-22 01:33:54:446:CNV: Message response sent  by Converter
5-12-22 01:33:54:446:CNV: MessageType                  :1110
5-12-22 01:33:54:446:CNV: Bitmap                       :FA7240010E30C000000000004016000000 bits:11111
5-12-22 01:33:54:446:CNV: F02_PAN                      :0000644444444444
5-12-22 01:33:54:446:CNV: F03_ProcessingCode           :310000
5-12-22 01:33:54:446:CNV: F04_AmountTransaction        :000000000000
5-12-22 01:33:54:446:CNV: F05_AmountReconciliation     :000000000000
5-12-22 01:33:54:447:CNV: F07_TransmissionDateTime     :1225013354
5-12-22 01:33:54:447:CNV: F10_ConvRateBill             :61000000
5-12-22 01:33:54:447:CNV: F11_SystemTraceAuditNumber   :200003
5-12-22 01:33:54:447:CNV: F12_DateTimeLocalTransaction :221226
5-12-22 01:33:54:447:CNV: F15_DateSettlement           :1224
5-12-22 01:33:54:447:CNV: F18_MerchantType             :5565
5-12-22 01:33:54:447:CNV: F32_AcquiringInstitutionIdenti:00007000000
5-12-22 01:33:54:447:CNV: F37_RetrievalReferenceNumber :235900200002
5-12-22 01:33:54:447:CNV: F38_ApprovalCode             :
5-12-22 01:33:54:448:CNV: F39_ActionCode               :14
5-12-22 01:33:54:448:CNV: F43_CardAcceptorNameLocation :JOHN DOE KITWE
5-12-22 01:33:54:448:CNV: F44_AdditionalResponseData   :
5-12-22 01:33:54:448:CNV: F49_CurrencyCodeTransaction  :967
5-12-22 01:33:54:448:CNV: F50_CurrencyCodeReconciliation:967
5-12-22 01:33:54:448:CNV: F90_OriginalDataElements     :2359002000039999999999999909785258350000000
5-12-22 01:33:54:448:CNV: F100_RecInstIdCode           :00006000000
5-12-22 01:33:54:448:CNV: F102_AccountId1              :9999999999999
5-12-22 01:33:54:448:CNV: F103_AccountId2              :4444444444
5-12-22 01:33:54:448:- - - - - - - - - - - - - - - - - - - - - - - - - - -
5-12-22 01:33:54:451:SYS:Set:MessageType:ascii:1110
5-12-22 01:33:54:451:SYS:Buffer added:31313130
```

Figure 13. Declined response 14 invalid account neaPay system log

PAYMENT & TRANSFER 1100

A transfer or payment 1100 authorization request is much like a KYC 1100 message with the main difference being that the processing code would be '030000' or '0400003 and the amount fields would not be populated with zeros but the amount to be transferred. for this 1100, the issuer is expected to authorize and credit receiver with un-cleared effect. Account entries is beyond scope of the simulations and hence not depicted here, however, the issuer was configured to respond with success and populating the necessary fields. Issuer echoes or received data fields and adds field 38 approval code, field 39 response code and field 44 the receiver's MCC. The figures 14, 15 and 16 show how data was populated in the acquirer interface, neaPay simulator and the issuer script. This was for a wrong account scenario. The figures 4-38, 4-39 and 4-40 show the scenario when the correct account is used.

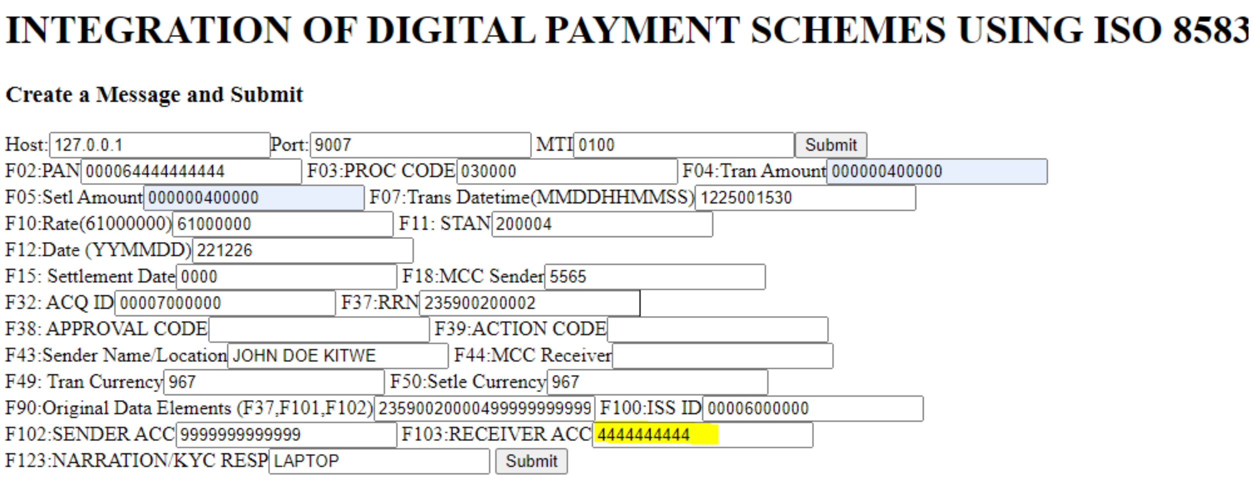

Figure 14. Transfer authorization request data wrong account

RESPONSE MESSAGE: □□1110□r@□□0□@□ 1500006444444444403000
KITWE 04 96796723590020000499999999999994444444444400000001100006
BITMAP:111110100111001001000000000000010000111000110000110000000

FIELDS:
MTI:1110
F02:000064444444444
F03:030000
F04:000000400000
F05:000000400000
F07:1225014513
F10:61000000
F11:200004
F12:221226
F15:1224
F18:5565
F32:00007000000
F37:235900200002
F38:
F39:14
F43:JOHN DOE KITWE
F44:
F49:967
F50:967
F90:235900200004999999999999944444444440000000
F100:00006000000
F102:9999999999999
F103:4444444444
F123:LAPTOP

Figure 15. Transfer authorization request response data-wrong account

```
25-12-22 01:45:13:492:CNV: Message response sent  by Converter
25-12-22 01:45:13:493:CNV: MessageType                    :1110
25-12-22 01:45:13:493:CNV: Bitmap                         :FA7240010E30C000000000004016000020 bits:1111101001110010010000000
25-12-22 01:45:13:494:CNV: F02_PAN                        :000064444444444
25-12-22 01:45:13:495:CNV: F03_ProcessingCode             :030000
25-12-22 01:45:13:495:CNV: F04_AmountTransaction          :000000400000
25-12-22 01:45:13:495:CNV: F05_AmountReconciliation       :000000400000
25-12-22 01:45:13:495:CNV: F07_TransmissionDateTime       :1225014513
25-12-22 01:45:13:495:CNV: F10_ConvRateBill               :61000000
25-12-22 01:45:13:495:CNV: F11_SystemTraceAuditNumber     :200004
25-12-22 01:45:13:495:CNV: F12_DateTimeLocalTransaction   :221226
25-12-22 01:45:13:496:CNV: F15_DateSettlement             :1224
25-12-22 01:45:13:498:CNV: F18_MerchantType               :5565
25-12-22 01:45:13:498:CNV: F32_AcquiringInstitutionIdenti:00007000000
25-12-22 01:45:13:498:CNV: F37_RetrievalReferenceNumber   :235900200002
25-12-22 01:45:13:498:CNV: F38_ApprovalCode               :
25-12-22 01:45:13:498:CNV: F39_ActionCode                 :14
25-12-22 01:45:13:498:CNV: F43_CardAcceptorNameLocation   :JOHN DOE KITWE
25-12-22 01:45:13:498:CNV: F44_AdditionalResponseData     :
25-12-22 01:45:13:499:CNV: F49_CurrencyCodeTransaction    :967
25-12-22 01:45:13:499:CNV: F50_CurrencyCodeReconciliation:967
25-12-22 01:45:13:499:CNV: F90_OriginalDataElements       :235900200004999999999999944444444440000000
25-12-22 01:45:13:499:CNV: F100_RecInstIdCode             :00006000000
25-12-22 01:45:13:500:CNV: F102_AccountId1                :9999999999999
25-12-22 01:45:13:500:CNV: F103_AccountId2                :4444444444
25-12-22 01:45:13:500:CNV: F123_Reserved                  :LAPTOP
25-12-22 01:45:13:501:- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 16. Transfer authorization response in neaPay system – wrong account

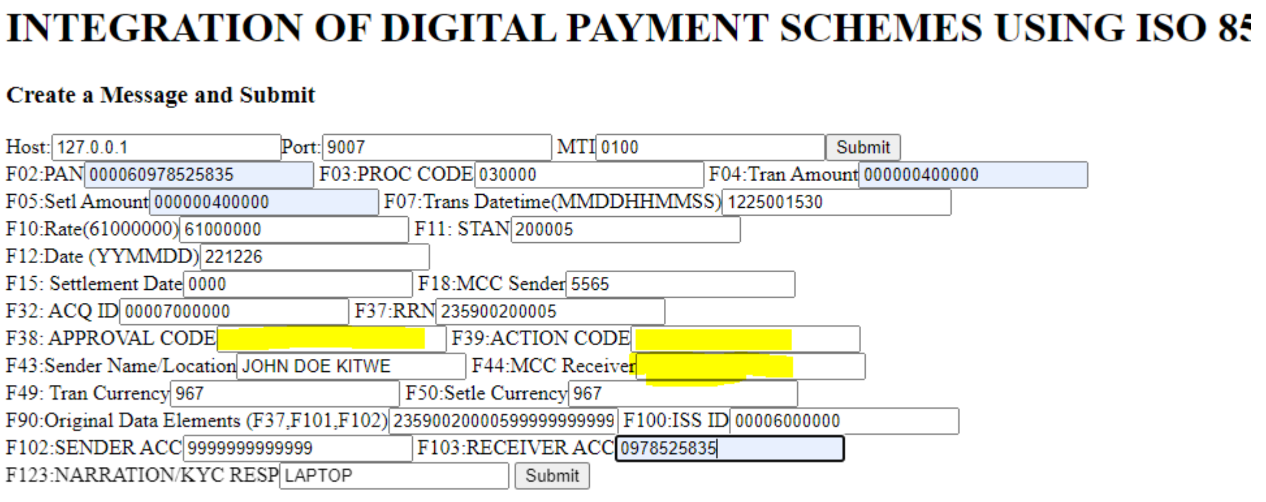

Figure 17. Transfer authorization request data correct account

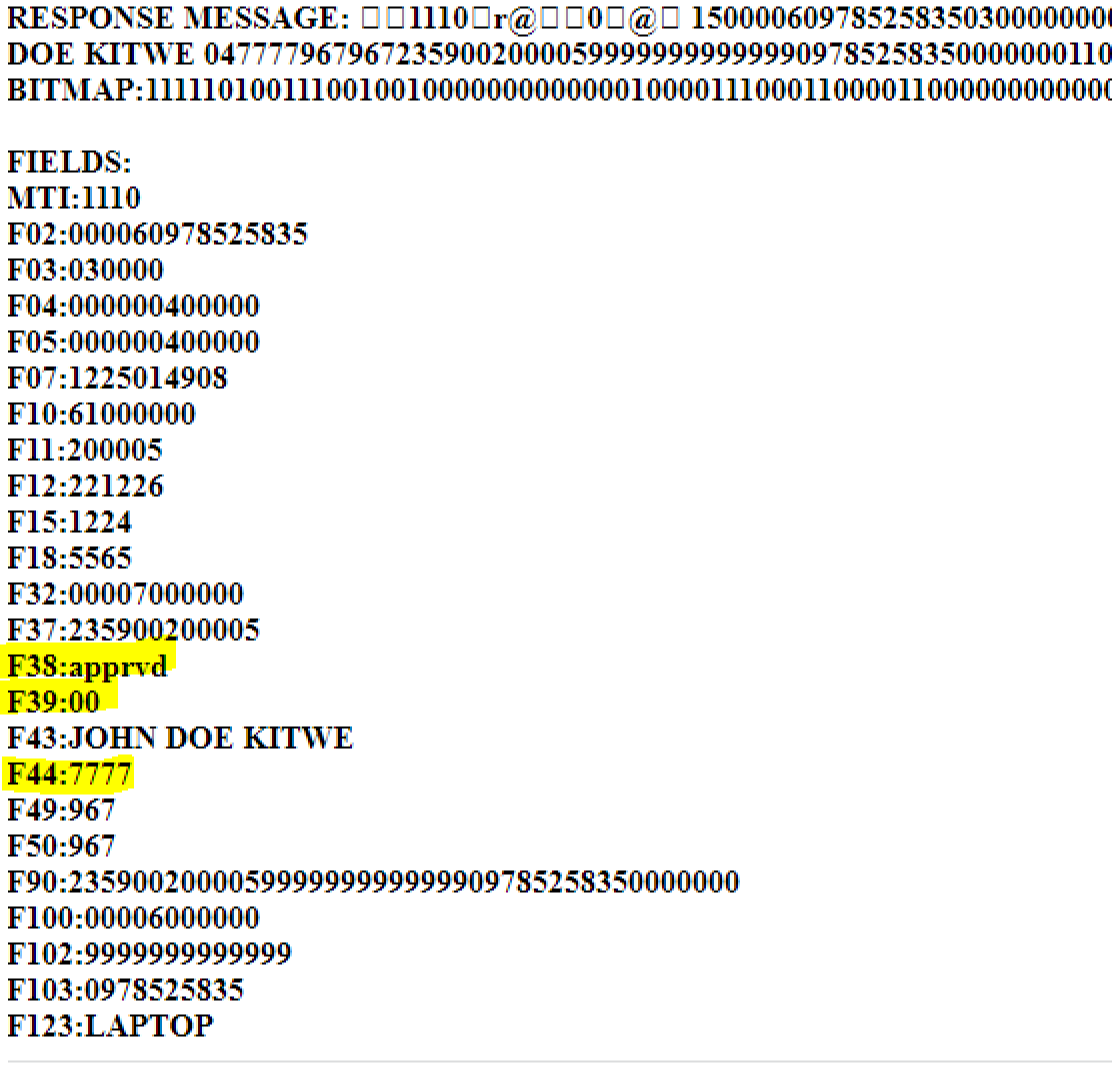

Figure 18. Transfer authorization request response data-correct account

```
25-12-22 01:49:09:095:CNV: Field:F127_ReservedPrivate| value:
25-12-22 01:49:09:095:CNV: Field:F128_MAC| value:
25-12-22 01:49:09:097:- - - - - - - - - - - - - - - - - - - - - - - - - - -
25-12-22 01:49:09:097:CNV: Message response sent  by Converter
25-12-22 01:49:09:097:CNV: MessageType                    :1110
25-12-22 01:49:09:097:CNV: Bitmap                         :FA7240010E30C000000000004016000020 bits:1111
25-12-22 01:49:09:098:CNV: F02_PAN                        :000060978525835
25-12-22 01:49:09:098:CNV: F03_ProcessingCode             :030000
25-12-22 01:49:09:098:CNV: F04_AmountTransaction          :000000400000
25-12-22 01:49:09:098:CNV: F05_AmountReconciliation       :000000400000
25-12-22 01:49:09:098:CNV: F07_TransmissionDateTime       :1225014908
25-12-22 01:49:09:098:CNV: F10_ConvRateBill               :61000000
25-12-22 01:49:09:099:CNV: F11_SystemTraceAuditNumber     :200005
25-12-22 01:49:09:099:CNV: F12_DateTimeLocalTransaction   :221226
25-12-22 01:49:09:099:CNV: F15_DateSettlement             :1224
25-12-22 01:49:09:099:CNV: F18_MerchantType               :5565
25-12-22 01:49:09:100:CNV: F32_AcquiringInstitutionIdenti:00007000000
25-12-22 01:49:09:100:CNV: F37_RetrievalReferenceNumber   :235900200005
25-12-22 01:49:09:100:CNV: F38_ApprovalCode               :apprvd
25-12-22 01:49:09:100:CNV: F39_ActionCode                 :00
25-12-22 01:49:09:101:CNV: F43_CardAcceptorNameLocation   :JOHN DOE KITWE
25-12-22 01:49:09:101:CNV: F44_AdditionalResponseData     :7777
25-12-22 01:49:09:101:CNV: F49_CurrencyCodeTransaction    :967
25-12-22 01:49:09:101:CNV: F50_CurrencyCodeReconciliation:967
25-12-22 01:49:09:103:CNV: F90_OriginalDataElements       :235900200005999999999999990978525835000000
25-12-22 01:49:09:104:CNV: F100_RecInstIdCode             :00006000000
25-12-22 01:49:09:104:CNV: F102_AccountId1                :9999999999999
25-12-22 01:49:09:105:CNV: F103_AccountId2                :0978525835
25-12-22 01:49:09:105:CNV: F123_Reserved                  :LAPTOP
25-12-22 01:49:09:105:- - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 19. Transfer authorization response in neaPay system – correct account

REFERENCES

[1] VISA (2017) Visa Innovations for a Cashless World 2017 report. Retrieved from: https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-innovations-for-a-cashless-world-2017-report.pdf.

[2] Bech, M. L., Faruqui, U., Ougaard, F., & Picillo, C. (2018). Payments are a-changin'but cash still rules. BIS Quarterly Review, March.

[3] Chishimba, M. B. (2022). Assessing the role of electronic payment systems in the promotion of financial services development in Zambia: case study of Lusaka (Doctoral dissertation, The University of Zambia).

[4] Financial Services Deepening (FSD) Zambia (2015), "FinScope Zambia,. from https://www.fsdzambia.org/publication/finscope-2015-zambia/.

[5] Bank of Zambia (2015), "National Payments Systems Annual Report" retrieved from https://boz.zm/payment-systems-annual-reports.htm.

[6] ZICTA (2018). ICT survey report individuals and households 2018. Retrieved from: http://www.zicta.zm/Views/Publications/2015ICTSURVEYREPORT.pdf.

[7] BOZ, Digital payments statistics (2019), https://www.boz.zm/payment-systems-statistics.htm.

[8] P. W. Ratan (2018), Digital Payments, Trends, Issues and Opportunities p. 9 Niti Aayog Publishing.

[9] AYDEN, (2022) Payments Methods in Zambia. https://www.adyen.com/payment-methods-guides/africa/zambia.

[10] Sahin, I. (2006). Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. Turkish Online Journal of Educational Technology-TOJET, 5(2), 14-23.

[11] Ha, N., & Nguyen, T. (2019). The effect of trust on consumers' online purchase intention: An integration of TAM and TPB. Management Science Letters, 9(9), 1451-1460.

[12] Poser, H. V. (2019). Facilitating the interoperability of high-value and international payments: The ISO 20022 migration of the Eurozone. Journal of Payments Strategy & Systems, 13(2), 113-120.

[13] Banerjee, D. A DETAILED ANALYSIS OF THE IMPACT OF ISO 20022 AS A NEW PAYMENTS STANDARD.

[14] Goswami, G. (2016). Effective Usage of ISO 8583 Messaging System in Payment Gateway and Order Fulfillment System on Online Shopping/E-Commerce Applications. ADBU Journal

of Engineering Technology, 4.

[15] Funcke, A. (2008). Incorporating an ISO 8583-service into an unreliable application.

[16] Knorr, M. (2022). Developments in industry standards for cross-border payments. Journal of Payments Strategy & Systems, 16(3), 283-291.

[17] Rosli, S. N., Anshari, M., Almunawar, M. N., & Masri, M. (2022). Digital Wallet Ecosystem in Promoting Financial Inclusion. In FinTech Development for Financial Inclusiveness (pp. 31-49). IGI Global.

[18] Atalay, T. (2020). E-commerce ecosystem: Fundamental concepts, business models and cybersecurity issue. International Journal of Business Ecosystem & Strategy (2687-2293), 2(2), 15-24.

[19] UNCDF, (2018). Are fintechs the key to achieving Zambia's financial inclusion targets by 2022? Retrieved from: https://www.uncdf.org/article/3375/are-fintechs-the-key-to-achieving-zambias-financial-inclusion-targets-by-2022.

[20] VISA Developer, (2022) debit card ecosystem: https://community.developer.visa.com/t5/Tutorials/A-Detailed-Look-at-the-Payments-Ecosystem-from-Visa-Payment/ba-p/7463.

[21] Visa, (2022) Overview of Payments & Card Product Solutions retrieved from https://partner.visa.com/site/learn/overview-of-payments.html.

[22] Clapper, D., & Richmond, W. (2016). SMALL BUSINESS COMPLIANCE WITH PCI DSS. Journal of Management Information & Decision Sciences, 19(1).

[23] de Luna, I. R., Liébana-Cabanillas, F., Sánchez-Fernández, J., & Muñoz-Leiva, F. (2019). Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. Technological Forecasting and Social Change, 146, 931-944.

[24] Kumar, A., Adlakaha, A., & Mukherjee, K. (2018). The effect of perceived security and grievance redressal on continuance intention to use M-wallets in a developing country. International Journal of Bank Marketing.

[25] Kwilinski, A., Volynets, R., Berdnik, I., Holovko, M., & Berzin, P. (2019). E-Commerce: Concept and legal regulation in modern economic conditions. Journal of Legal, Ethical and Regulatory Issues, 22, 1-6.

[26] GSMA, Integrating mobile money and e-commerce: what are the challenges to overcome? Retrieved from https://www.gsma.com/mobilefordevelopment/programme/mobile-money/integrating-mobile-money-e-commerce-challenges-overcome/.

[27] Chitakala, C., & Phiri, J. (2022). Factors that Affect SMEs in the Adoption of E-Tax Payment Systems in Zambia, the Case of Kamwala Trading Area-Based on UTAUT Model. Open Journal of Business and Management, 10(6), 3395-3408.

[28] Ann Kjos* (2007), The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges retrieved from https://philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2007/D2007OctoberMerchantAcquiring.pdf.

[29] Amilan, S., & Aparna, K. (2021). Role of perceived countries' advantages of cashless economy in behavioral intentions of using cashless transactions: an empirical analysis. Journal of Indian Business Research.

[30] Doheir, M., Talib, M. S., Harum, N., Abu, N. A., Al-Mhiqani, M. N., & Ali, M. F. (2019). Impact of cashless society on the economic growth in Malaysia. RELIGACIÓN. Revista de Ciencias Sociales y Humanidades, 4(16), 300-307.

[31] Hutchinson, M. L., Isenstein, L. M., Goodman, A., Hurley, A. A., Douglass, K. L., Mui, K. K., ... & Zahniser, D. J. (1994). Homogeneous Sampling Accounts for the Increased Diagnostic Accuracy Using the ThinPrep™ Processor. American journal of clinical pathology, 101(2), 215-219.

[32] World Bank (2022) "Rural Population (% of total population-Zambia)" retrieved from https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS?locations=ZM.

[33] ZECHL, (2015) ISO 93 External Interface Specification - Amendments Phase II V1.3_emone... (1).pdf.

[34] ZECHL, (2021) E-Money ISO 93 External Interface Specification - V2.4 (1).pdf.