"A System and Method for Preparing Parties for a Financial Transaction"

Field of the Invention

This invention relates to financial transactions between parties involving a merchant with point-of-sale facilities to prepare for and submit the transaction for processing by a financial service provider. The invention has particular, although not exclusive, utility with respect to effecting money transfers between parties at high traffic flow retailers such as convenience stores.

The following indicative, but not exhaustive, definitions apply to the use of the indicated terms throughout the specification:

a "financial transaction" is defined to mean any form of transaction between parties involving compliance or regulation or both, and includes an agreement, communication or movement carried out between a merchant and a customer to exchange an asset for payment, registration of an account or customer that will be later used for regulated activity, a money transfer, opening a bank account, opening a stock broking account, activating a phone or mobile phone account, etc.

a "financial service provider" is defined to mean an organisation that manages money and includes a money transfer provider, credit union, bank, credit card provider, insurance provider, accountancy provider, consumer finance provider, stock brokerages, investment funds, and telephone company, a utilities service provider, and certain government sponsored enterprises.

a "merchant" is defined to mean any person or entity involved in trade, including both wholesale and retail trade and includes retailers and convenience store retailers.

"AML/CTF legislation" is defined to mean Anti-Money Laundering and Counter-Terrorism Financing legislation or similar in a country or region, which in Australia is the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and in the USA is the Dodd-Frank Wall Street Reform and Consumer Protection Act.

"money laundering" is defined to mean the process of concealing the source of money obtained by illicit means, and moving that money in the financial system as legitimate funds.

"terrorism financing" is defined to mean the financing of terrorist acts, terrorists and terrorist organisations.

a "regulator" is a person or authority responsible for regulating financial transactions and money transfers under relevant AML/CTF legislation.

"KYC policy" is defined to mean a 'Know Your Customer' policy which sets out a business' approach to ensuring that it can effectively identify, verify and monitor its customers and the financial transactions in which they engage, relative to the risks of money laundering and terrorism financing. For example, KYC policy in Australia has five major elements: customer acceptance, customer identification, customer verification, accounts and transactions monitoring and risk management.

a "compliance program" is defined to mean a merchant's statement of compliance in accordance with a KYC policy or similar as required under AML/CTF legislation.

"business rules" of a merchant are the rules stated in the compliance program and can be combined with any other rules a merchant may wish to be imposed on a counter operator of the merchant

"compliance triggers" are defined in the compliance program and are embedded in a governing host that forms part of the invention.

a "compliance report" is defined to mean a report that is compiled by the governing host based on compliance triggers.

a "compliance officer" is defined to mean a merchant's nominated representative for administering the compliance program.

Also throughout the specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Background Art

The following discussion of the background art is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was part of the common general knowledge as at the priority date of the application.

High traffic flow retailers such as convenience store retailers must have a fast counter transaction time. Unlike banks or post offices, the customer expectation is fast service.

Financial transactions normally require a number of reasonably complex validation and compliance processes to be performed by staff when performing financial transactions involving financial institutions. These transactions are regulated under KYC and AML/CTF legislation that apply to transactions involving financial institutions, professionals working within the financial sector, bullion and gambling sectors as well as other regulated entities. For example, they include financial transactions involving depositing and lending of money, insurance, phone accounts, international money transfer, lotteries, opening of accounts, transferring of money between accounts and for money transactions. Consequently staff members have generally required a high level of skill and training to perform financial transactions over the counter. This tends to run counter to the business model adopted by most convenience stores, which is focused on low level skill and training requirements and very low numbers of staff.

Convenience stores are not accustomed to high levels of compliance, fraud and cash management risk. They are also not able to hold large amounts of cash in the till due to the risk of robbery.

Consequently, convenience store retailers adopt a business model where all transactional activity is incorporated into their Point of Sale (POS) systems in preference to stand-alone systems that create difficulties when balancing and reconciling store activity. For example, transactions involving lottery win payouts or sales are most often managed in a separate stand-alone system to the POS system because POS integration is too difficult. This means that the retailer has to

match transactions that the lottery terminal specifies occurred with transactions that the POS terminal specifies occurred, creating another layer of complexity and time consuming activity for the retailer. System integration projects that are undertaken to overcome some of these problems are usually complex, expensive and time consuming.

Given the problems mentioned above, convenience store retailers have used various systems for performing financial transactions, each having their own drawbacks in one form or another. These include:

1. Paper based forms - The advantage of paper based forms systems is that they are low cost. Disadvantages are that they are slow and require a high level of staff training. They tend to fail in the convenience store environment mostly due to slow transaction times and the lack of integration with POS systems. Complex training requirements means long implementation cycles; and long transaction times at the store counter means that complex financial transactions cannot be done in high traffic convenience store environments.

2. POS data entry - The advantage of this form of entry is that the transaction can be completed successfully at the counter. Disadvantages are that it is slow and requires a high level of staff training. It tends to fail in the convenience store environment mostly due to slow transaction times. As with paper based forms, complex training requirements means long implementation cycles.

3. Staging the transaction with a telephone request followed by POS completion - The advantage of this system is the staging of transactions which reduce the time that the customer needs to spend at the counter occupying a counter operator. The disadvantages are that the system requires extensive use of a call centre and language difficulties can make the data collected inaccurate. It fails in a convenience store environment due to lack of customer acceptance of this method, the costs of running a helpdesk, complex training requirements, which translate into long implementation cycles.

4. Complete self-service solution on an ATM or other device that can take payment - The advantage is that there is no problem with counter time. Disadvantages are high capital costs of hardware and difficulty verifying customer identity for compliance purposes. It fails in a convenience store environment due to:

    - high capital costs and cash collection and management costs;
    - the lack of integration with POS systems and long implementation cycles; and
    - the fact that consumers do not feel comfortable handing their money to a machine.

5. Automated form-fill solutions that are married with a counter device provided by a financial service provider (FSP) - whilst such solutions meet validation and compliance requirements for the FSP to discharge its responsibilities they provide little help to the retailer to discharge its compliance obligations, or manage fraud and compliance risk or enforce granular business rules. These solutions still require a counter operator to be comprehensively trained and to make decisions on whether KYC and AML legislation applies to sometimes complex patterns of transactions that are presented to the retailer. Consequently, these systems are not sufficiently bespoke to help the merchant meet its validation, compliance and fraud detection requirements in a way that is operationally practical.

Reducing revenues in core categories such as cigarettes and petrol puts pressure on convenience store merchants to offer more extensive service offerings. Some of these categories involve financial transactions which have training requirements and counter processes for merchants and their staff alike that run counter to the high traffic flow, fast paced business model which has been the foundation of their success.

One of the seminal problems that needs to be overcome is that the onus is presently on the merchant or staff member to review transaction histories of customers and decide themselves as to what is suspicious and potentially

fraudulent activity and what is not in advance of or whilst a transaction is in progress.

Disclosure of the Invention

It is an object of the present invention to overcome or mitigate at least some of the problems identified above associated with the performance of reasonably complex financial transactions involving a merchant and customer that are capable of being performed in a high consumer flow retail environment.

In accordance with one aspect of the present invention, there is provided a financial transaction system for preparing parties for a financial transaction to be processed by a financial service provider, including:

a governing host having a database for registering the parties wishing to perform a financial transaction between them using the financial service transfer provider to ultimately process the financial transaction;

a discrete terminal independently accessible by one of the parties wishing to initiate a financial transaction with another of the parties and for communicating with the governing host to prepare for the transaction, the discrete terminal having a local transaction process providing for the initial validating and enforcing of business rules governing the transaction with the one of the parties and to generate a transaction key confirming that the initial validating and enforcing has been successful to complete a first preparatory stage of the financial transaction and that a second preparatory stage of the transaction is authorised by the governing host to proceed;

a facilitator device for completing the second preparatory stage of the financial transaction at a point-of-sale terminal of the other of the parties, the facilitator device having a reader to read the transaction key on being supplied with same from the one of the parties and communicate with the governing host to complete the second preparatory stage of the transaction using the point-of-sale terminal;

the discrete terminal being located separately of the point-of-sale terminal and capable of being accessed and operated independently by the one of the parties,

offline of any point-of-sale activity involving the point-of-sale terminal and the facilitator device;

the facilitator device including a facilitator process to instruct the other of the parties on those steps required to complete the second preparatory stage of the transaction in a manner that facilitates final compliance with the business rules governing the transaction and other requirements of the other of the parties;wherein the discrete terminal and facilitator device are able to validate or reject the transaction having regard to compliance with the business rules governing the transaction that are required to be performed by the other of the parties during the first or second preparatory stages of the financial transaction respectively.

Preferably, the facilitator device is integrated into the point-of-sale terminal.

Preferably, the local transaction process includes a customer registration process, a send money transaction process, a receive money transaction process, or a foreign exchange enquiry process.

Preferably, the facilitator process includes prompting the other of the parties to conduct an identity check of the one of the parties and validating the transaction for submitting to the financial service provider only after the other of the parties has verified completion of the identity check.

Preferably, the governing host includes fraud detection means including a fraud checking process to analyse patterns of transactions that may be fraudulent or non-compliant and to alert when detecting same.

Preferably, the facilitator process creates a record of the financial transaction for submitting to the financial service provider only after the other of the parties has verified the conduct of the identity checks and the financial transaction has been further validated by the governing host.

Preferably, the governing host includes a compliance framework to enforce compliance requirements with the one party dependent on the business rules that need to be complied with by the other of the parties during the first and second preparatory stages of the transaction, before submitting the financial transaction

for processing by the financial service provider, in response to communication with the discrete terminal as part of the local transaction process.

Preferably, the governing host includes a compliance monitoring process including a trigger setting process for setting compliance trigger limits that define the compliance framework of a merchant and a transaction examining process to ensure compliance with the business rules of the merchant.

Preferably, the transaction examining process further ascertains whether a compliance trigger limit has been breached suggesting a money laundering, terrorist financing or fraudulent activity and invoking a prescribed contingency process.

Preferably, the prescribed contingency process includes a stop process to stop any further transacting occurring after a set limit of a compliance trigger is reached, an alert process to launch an investigation process when a particular predefined compliance trigger has stopped a transaction, and a compliance report process to compile and send a compliance report.

Preferably, the financial transaction system includes a products and services handling infrastructure to allow third party products and services to be supplied to a customer on the discrete terminal and constitute a financial transaction prepared by the financial transaction system by way of the discrete terminal and facilitator device for compliance and validation in accordance with the business rules of the merchant before being submitted to the financial services provider for processing.

Preferably, the financial transaction system includes a training setting process for defining counter operators of the merchant and to set counter operator training status for use in enabling operation of the facilitator device so that only trained operators are able to use the facilitator device.

Preferably, the governing host includes logging means that applies an operator stamp listing a store identifier, the counter operator identifier and their training status to a log of financial transactions performed using the facilitator device.

In accordance with another aspect of the present invention, there is provided a method for preparing parties for a financial transaction to be processed by a financial service provider including:

registering one of the parties for performing a financial transaction offline from any point-of-sale activity;

receiving a request from a registered party wishing to initiate a particular type of financial transaction with another of the parties offline of any point-of-sale activity involving the other of the parties;

communicating with a governing host to prepare for the transaction during a first preparatory stage for providing for the initial validating and enforcing of business rules that need to be complied with by the other of the parties governing the transaction, involving interaction with the one of the parties;

generating a transaction key for the one of the parties and storing the transaction key on the governing host on validating the first preparatory stage of the transaction;

completing a second preparatory stage of the financial transaction at the point-of-sale on the other of the parties being provided with the transaction key by the one of the parties, including:

(i) communicating with the governing host and prompting the other of the parties to further validate the transaction in accordance with the compliance requirements of the other of the parties as determined by the governing host; , and

(ii) submitting the financial transaction with the financial service provider at point-of-sale for processing after communicating with the governing host as appropriate to further validate the transaction.

Preferably, the step of receiving a request from a registered party occurs locally of the other of the parties but offline of any point-of sale activity involving the parties.

Preferably, the method including submitting the financial transaction for processing by the financial service provider only after prompting the other of the

parties to conduct identity checks of the one of the parties based on the delivery of instructions to the other of the parties by the governing host.

Preferably, the method including applying the business rules of the other of the parties as part of the initial validating and enforcing performed during the first preparatory stage.

Preferably, the method including the local transaction process receiving alerts of fraudulent or non-compliant transactions from the governing host, analysing the request having regard to same, and alerting when detecting same.

Preferably, the method including creating a record of the financial transaction for submitting to the financial service provider only after the other of the parties has verified the conducting of the identity checks.

Brief Description of the Drawings

The drawings referred to in the Best Mode(s) for Carrying Out the Invention are as follows:

Fig.1 is a structural block diagram showing the structure of the financial transaction system;

Fig. 2 is a flowchart showing an overview of the money transfer process that can be performed using an electronic kiosk and counter operator staff of the merchant;

Fig. 3 is a flowchart showing the customer registration/ foreign exchange enquiry process;

Fig. 4 is a flowchart showing the reconciliation transaction process;

Fig. 5 is a flowchart showing the send money transaction process;

Fig. 6 is a flowchart showing the receive money transaction process;

Fig. 7 is a flowchart showing the customer registration process;

Fig. 8 is a flowchart showing the enquiry transaction process;

Fig. 9 is a flowchart showing problem resolution transaction process;

Fig. 10 is a flowchart showing the network management transaction process; and

Fig. 11 is a flowchart showing the network upgrade transaction process.

Fig. 12 is a block diagram showing the compliance/fraud monitoring engine and other background tracking and handling processes;

Fig. 13 is a flowchart showing the business process flow of the generalised products and services handling infrastructure;

Fig. 14 is a block diagram showing the interaction of the various components of the financial transaction system to create the infrastructure for generalised products and services handling; and

Fig. 15 is a flowchart showing the process flow for defining an administrator and counter operator for a merchant and recording training status for facilitator device use.

Best Mode(s) for Carrying Out the Invention

The best mode for carrying out the invention is described according to one specific embodiment. The embodiment is directed towards a financial transaction system 11 for preparing parties for a transaction to be processed by a financial service provider or a money transfer provider (FSP), effectively comprising three discrete systems communicating with each other via a governing host using a network in the form of the Internet 13. It should be appreciated that in other embodiments a dedicated LAN or WAN network can be used other than the Internet.

The financial transaction system 11 is specifically adapted to service a chain of convenience store merchants 15 where each convenience store has a standard point-of-sale (POS) terminal 17 manned by a counter operator staff member of the merchant for serving customers 19. For the purposes of the ensuing description of the system, the merchant and counter operator staff member will be treated synonymously and will be referred to as facilitators who facilitate completing the performance of the financial transaction, either generally or individually by the reference numeral 15.

The financial transaction system 11 includes:

- a governing host 21 operated by a host administrator/manager 20 that is remotely located of the convenience stores and their facilitators 15 in the cloud via the Internet 13 and has a database 22 for registering parties wishing to perform financial transactions with particular merchants;

- a discrete terminal in the form of a self-service electronic kiosk 23 and printer 24 located in each convenience store 15 to communicate with the governing host via the Internet 13 and having a local transaction process for initially preparing a financial transaction with a customer; and

- a facilitator device 25 having a scanner 27 and printer 29 provided at the point-of-sale area of the store such as the sales counter for use by the counter operator staff member 15 and having a facilitator process to facilitate and complete the preparatory processing of the financial transaction with a customer 19 who has used the services provided by the electronic kiosk 23.

Once the financial transaction has been validated by the facilitator device, the counter operator staff member can then submit the financial transaction to the FSP using the store's POS terminal 17.

In the present embodiment, the principal services provided by the electronic kiosk 23 to the customer 19 involve complex electronic financial transactions, including international money transfers to facilitate the customer paying for a transfer or receiving funds transferred to them, all through the agency of the financial transaction system 11 and the convenience store as necessary on the one hand, and an FSP on the other hand.

By using a self-service electronic kiosk 23, a facilitator device 25 and a set of applications provided by the governing host 21, the financial transaction system 11 is designed to stage a financial transaction in two preparatory steps:

- firstly the customer 19 prepares for a transaction at the self-service electronic kiosk 23 independently and offline of any point-of-sale activity involving the POS terminal 17, by the kiosk obtaining relevant details from the customer and validating the first preparatory stage of the transaction, enforcing part of the required business rules governing the transaction that

a merchant needs to comply with in accordance with KYC policy under AML/CTF legislation, and producing a kiosk transaction key verifying same;

- then secondly the preparation of the transaction is completed at the store counter by the counter operator staff member 15 during the second preparatory stage, on the counter operator being provided with the kiosk transaction key by the customer, making the mandatory physical checks to complete adherence to KYC policy requirements to facilitate compliance with the remainder of the business rules governing the transaction in a manner that is similar to, and is as simple as, selling a packet of cigarettes.

In this manner, both the kiosk 23 and the facilitator device 25 are able to validate or reject the transaction having regard to compliance with the business rules governing the transaction that are required to be performed by the merchant, during the first preparatory or the second preparatory stage of the financial transaction, before the financial transaction is presented for processing by the POS terminal 17.

By virtue of adopting this staged approach for preparing for the financial transaction and the particular configuration of the financial transaction system 11 described, involvement of the counter operator staff member 15 in performing financial transactions can be kept to a minimum whilst ensuring compliance requirements of the merchant with the business rules governing the transaction are facilitated and optimised.

The applications provided by the governing host can also involve complex fraud detection and sophisticated inventory tracking software that normally would not be available to the merchant and can be provided as cloud based services. Thus in the present embodiment, the financial transaction system 11 includes fraud detection means having a fraud checking process on the governing host 21 and a fraud detection client application 24 operating on the electronic kiosk 23 communicating with the fraud checking process to analyse patterns of transactions that may be fraudulent or require further regulatory compliance action and to alert a compliance officer when detecting same.

Before describing the functional and technical aspects of the embodiment in detail, some of the issues associated with complex financial transactions that the financial transaction system of the present embodiment addresses will be described first to gain a better appreciation of the innovative aspects of the invention.

Compliance Monitoring Automation

International money transfers are regulated by government authorities in every country. The majority of governments take their Anti Money Laundering and Counter Terrorist Financing (AML/CTF) legislation and business rules from recommendations by the Financial Action Task Force (FATF) an inter-governmental body established in 1989 by the Ministers of its Member Jurisdictions.

The recommendations result in compliance requirements for each organisation involved in financial services that fall under the AML/CTF legislation and are manifested in agreed to business rules that need to be followed and complied with in order to meet the requirements of the AML/CTF legislation. These compliance requirements can be quite onerous and time consuming to manage. There are usually serious penalties for non-compliance.

For example, in Australia, AML/CTF legislation requires an organisation involved with financial services to adopt a KYC policy. As defined above, KYC policy in Australia has five major elements: customer acceptance, customer identification, customer verification, accounts and transactions monitoring and risk management.

Customer acceptance is the point at which a new customer is accepted or rejected and is the easiest point at which the risk of dealing with illegal money can be avoided. By following good customer acceptance policies, dealing with entities and individuals who might engage in illegal transactions can be avoided.

Customer identification involves establishing the identity of a customer both for the customer acceptance or rejection decision and for the ongoing monitoring of customer accounts and transactions. By identifying customers effectively, the business is able to deal with them in the appropriate manner.

Customer verification involves verifying that a customer is who they say they are and is vital to any customer identification procedure. Merely collecting customer information is not enough for an effective KYC policy. Reliable and independent documentation should be used to support and confirm the identification details a customer provides; for example, citing an original primary photographic identification document such as a passport or drivers licence.

Accounts and transaction monitoring involves properly classifying customer accounts and transactions in terms of risk and regularly monitoring customer activity through checks and enforcing thresholds. In this manner, unusual activities, activities by high-risk customers, or suspicious behaviour can be detected and reviewed.

Risk management ensures that the risks posed by money laundering and other criminal activities are identified, mitigated and managed. Good risk management practices are set out in the Australian Standard on Risk Management: AS4360.

Whilst the specifics of KYC policy vary a little from market to market, the tenets of the policy are essentially the same throughout the world.

Convenience store retailers that offer money transfer services such as would be the case with merchants of convenience stores in the present embodiment are responsible for the monitoring of customer activity and performing the appropriate level of customer due diligence on their money transfer transactions in order to comply with these compliance requirements through a KYC policy. In addition to monitoring individual stores, the merchant is also responsible for monitoring activity across the store network.

The regulations setting out compliance with KYC policy are updated from time to time, often driving operational changes that a convenience store retailer is unable or unwilling to execute.

In the US, the introduction of new legislation such as the Dodd-Frank Wall Street Reform and Consumer Protection Act can have a material impact on the way that a business must manage a financial transaction. For example, under Dodd-Frank provision was required for terms and conditions and product disclosure statements being presented in multiple languages prior to the kiosk transaction

being concluded. Thus legislative change drives operational change that a retailer is unable or unwilling to execute.

Another source driving change is judgements from regulators against FSP's and operators highlighting inadequate compliance. Such judgements often require tightening of processes and systems to meet compliance that a retailer is unable or unwilling to execute.

The financial transaction system 11 provides a methodology for capturing activity in a manner that facilitates on-going monitoring of customer transactions in accordance with a prescribed set of business rules of a merchant to meet compliance obligations in accordance with KYC policy under AML/CTF legislation, and includes a compliance monitoring process to perform this monitoring on an immediate, weekly and monthly basis. This ensures that the merchant is meeting their AML/CTF obligations in a comprehensive and time efficient manner.

Importantly, this methodology enables the governing host 21 to implement any new changes to KYC policy or other compliance obligations under AML/CTF legislation by modifying the business rules of the merchant as required, and driving these changes to the customer via local transaction processes on the electronic kiosk 23, leaving facilitator transaction processes largely intact.

The compliance monitoring process is implemented in the governing host 21 and will be described in more detail later.

Fraud Alerts

Money transfer is a target for fraud as funds are moved quickly and irrevocably. Fraud by staff members of the merchant or by customers of the merchant can be costly. The merchants (store owners) need to have confidence that there are processes in place to identify and halt fraudulent transactions.

The financial transaction system 11 includes the fraud checking process for monitoring transactions in real time to identify and halt potential fraud by establishing customer and store fraud rules and halting transactions if customers or stores exceed the fraud limit parameters. The fraud checking process is implemented in the governing host 21 and communicates with the fraud detection

client application as previously described to monitor transactions prepared at the kiosk and includes an alert process for providing immediate alerts and a daily summary that identifies transactions that could constitute possible instances of fraud. In this manner, compliance events are monitored by the governing host 21 and thus complex regulatory decisions do not need to be made by operators or counter operator staff members at the point-of-sale at the merchant's premises, as is the case with prior art systems.

The fraud checking process will be described in more detail later.

Customer conversion analytics and automated response

International money transfer is a competitive business where customers shop around for the best deal. Merchants 15 have not been able to determine if the sales volumes are being negatively impacted by competitive action. The merchant also needs to determine pricing, but is not normally able to see the sales impact of price increases or decreases at a detailed level.

The financial transaction system 11 includes a sales tracking process for tracking the number of quotes against the number of transactions to arrive at a conversion rate. This conversion rate is tracked for specific "corridors" such as the sending country to the receiving country for a particular store, group of stores, region or whole business during a specified time period and provides a report of this to the merchant. By examining the conversion rate over time, the merchant can determine where pricing adjustments need to be made.

The sales tracking process is also implemented in the governing host 21 and will be described in more detail later.

Lost customer analytics and automated response

The majority of international money transfer customers transact regularly. Some are one time users, and some are occasional users of the service. Merchants are not able to determine when a regular customer stops transacting, so these valuable customers just disappear.

The financial transaction system 11 has a customer tracking process for identifying regular customers that have stopped transacting and automatically

generates a targeted offer, such as a discount, coupon or other incentive, to attract the customer to return. The system 11 also includes a customer tracking monitoring process for monitoring the effectiveness of this program by tracking the customers that do return.

The customer tracking process and customer tracking monitoring processes are both implemented on the governing host 21 and will be described in more detail later.

Generalised products handling

Products and services that are offered to customers via an in-store electronic kiosk and facilitator device of the type described in the present embodiment would normally pose a significant problem to merchants updating the product name and changing the counter operation process performed by the counter operator staff member. This would normally take a full software development, testing and distribution process that is time consuming and also costly for merchants.

The financial transaction system 11 includes a generalised products handling infrastructure, which allows for third party products and services to be configured on the system. Instructions for store operator transaction handling are determined by this particular product and services configuration, which can be centrally maintained on the governing host 21 and operated via the electronic kiosk 23.

The generalised products and services handling infrastructure is implemented on the governing host 21 and electronic kiosk 23 and will be described in more detail later.

Specific Embodiment

As indicated, each of the aforementioned problems are overcome by the financial transaction system 11 of the present embodiment and in particular its configuration and processes that have been developed with the aforementioned problems in mind.

The particular functionality of each of the aforementioned systems making up the financial transaction system 11 that enables fast and simplified processing of complex financial transactions of the type described will now be described.

The self-service electronic kiosk 23 has a local transaction process that when operated effectively performs three functions invoked by discrete processes during the first preparatory stage of performing a financial transaction including:

(i) enforcing of validation and business rules governing a financial transaction with which a merchant needs to comply when a customer registers their details and processes their transaction request at the kiosk terminal preparatory to making a financial transaction with a financial service provider, separate from any interaction with the counter operator staff member at the counter of the convenience store;

(ii) storing customer details and transaction request details on the governing host 21 with which it communicates via the Internet 13;

(iii) producing a voucher 31 with a kiosk transaction key in the form of a unique barcode in respect of the financial transaction performed at the electronic kiosk 23 for the customer to take to the store counter and for the counter operator staff member of the merchant to process the order to complete the transaction.

The governing host 21 also performs three principal functions. It includes governing processes for:

(i) enforcing validation and business rules of a merchant governing the transaction with which a merchant needs to comply when a transaction is processed by it from a self-service electronic kiosk 23 during the first preparatory stage of performing a financial transaction by virtue of an initial compliance monitoring process;

(ii) using the information gathered from the self-service electronic kiosk 23 to complete compliance requirements associated with the transaction via interaction with the facilitator device 25 at the counter of the convenience store during the second preparatory stage of performing a financial transaction by virtue of a final compliance process; and

(iii) building a comprehensive database of customer interactions for marketing, business risk management and compliance purposes by virtue of the sales and customer tracking processes and generalised products handling process.

The facilitator device 25 similarly includes the facilitator process that when operated effectively performs five principal functions that:

(i) identify the transaction key by reading the barcode voucher 31 produced at the electronic kiosk 23 by the customer 19, by way of the scanner 27 when the customer is served and presents the voucher during the second preparatory stage of performing the financial transaction;

(ii) instruct the convenience store counter operator staff 15 on the remaining compliance and processing steps that need to be performed to complete the financial transaction and verify the business being done;

(iii) produce a sales receipt 33 using the printer 29 that has the financial service provider reference number and which is given to the customer 19 as part of the financial transaction involving the merchant;

(iv) generate a POS transaction key 34 which is used to complete the financial transaction with the FSP at the convenience store point-of-sale terminal 17; and

(v) receive a transaction identifier which confirms completion of the financial transaction with the FSP and provides a POS transaction identification that binds the transaction to a POS transaction file for matching during the settlement process.

Additional functions and features included within the financial transaction system 11 that combine to make the system work in a convenience store environment to overcome the aforementioned problems are numerous. These include:

- self-service aspects that enable customers to successfully use the system without training;
- merchant features that enable complex financial transactions to be performed in a convenience store environment; and
- system management capabilities that ensure high system availability and remote support efficiency

In the case of self-service aspects, the system is able to provide for:

(i) multi-lingual screen prompts to come up from which customers can select from a number of different languages;

(ii) the subsequent presentment of terms and conditions in the selected language;

(iii) the adoption of a simplified customer identification being the customer's mobile number or email address;

(iv) the customer determining their password at the time that they register with the system 11 when at the self-service electronic kiosk 23;

(v) when a customer forgets their password, a facility of automatically sending a new password to the customer's mobile phone and/or email address upon correctly answering a security question previously established during the registration process;

(vi) presenting the customer with a changeable screensaver that communicates current promotions of the convenience store or other messages;

(vii) timing out customer sessions after a nominated timeframe which varies according to the function they are using whereupon the system is reset to commence a new transaction;

(viii) facilitating customer operation of the electronic kiosk 23, by the kiosk having a touchscreen keyboard that disables characters which are not valid for the specific field the customer is entering;

(ix) the kiosk having a help button that allows the customer to access to a video presentation that shows an overview of how to operate the system;

(x) the customer having access to a helpdesk operator 30 as part of the services provided by the governing host 11, where the operator can view and remotely control the touchscreen on the kiosk to assist the customer when asked.

With respect to merchant features, these include:

(i) validating the first preparatory stage of the transaction as part of the process that the customer undertakes at the electronic kiosk 23, which means that the counter operator staff do not need to perform these validation activities;

(ii) the governing host 21 performing fraud checking in accordance with the merchant's specific fraud profile on any financial transaction performed by a customer at the electronic kiosk 23 and blocking transactions from being processed if they do not comply with the fraud profile without necessitating involvement of the merchant;

(iii) the governing host 21 performing compliance checking, monitoring and reporting on an on-line basis daily, weekly and monthly;

(iv) the governing host 21 processing settlement thereby ensuring that each transaction is balanced between the store systems of the merchant and the host systems;

(v) the governing host 21 performing a detailed logging of all system activity to enable error detection and correction;

(vi) the governing host 21 performing a detailed marketing analysis enabling both the merchant and supplier of the financial transaction

system 11 to improve outcomes of the operation of the convenience store by identifying trends and potential problem areas;

(vii) the electronic kiosk 23 providing for counter operator staff training when required;

(viii) the financial transaction system 11 continuously monitoring potential fraudulent behaviour patterns and trigger live alerts to mobile phones, email addresses for immediate action in response to detecting any such behaviours;

(ix) the loading of a prepaid debit card at the facilitation device 25 supplied to the customer that can be redeemed at an ATM for the customer receiving funds beyond a prescribed limit available from the convenience store to avoid the merchant having to hold large amounts of cash in the till.

With respect to system management capabilities these include:

(i) the governing host 21 monitoring all electronic kiosk 23 and facilitator devices 25 to ensure they are operational;

(ii) the governing host 21 monitoring all printers connected to the electronic kiosk 23 to ensure they are operational;

(iii) the governing host 21 remotely distributing software updates to the electronic kiosk 23 and facilitator devices 25;

(iv) integrating all system alerts, helpdesk emails and helpdesk phone calls into one issue management system handled by the governing host 21;

(v) the provision of remote support and operation of the electronic kiosk 23 via the governing host 21 while a customer is using the kiosk.

In order to perform these functions and processes, the governing host 21 generally comprises a centralised server and database 22 which manages and controls the delivery of instances of all money transfer transactions being prepared at each electronic kiosk 23 connected to it via the Internet 13.

Furthermore, the governing host 21 is able to configure each electronic kiosk 23 by downloading a compliance framework stored on the database 22 customised for each merchant to define their own set of business rules. The compliance framework allows the governing host 21 to manage the interactions between the kiosk 23 and the customer 19 on an ongoing basis, and update the compliance framework when necessary, at appropriate times in response to KYC policy changes driven by legislative or regulator change. Importantly, this compliance framework governs the interaction in a way to ensure that the right data elements for meeting compliance with the business rules of the merchant are presented in the right way to the customer, eliminating or at least substantially mitigating the risk of counter operator error during preparation of a financial transaction.

The basic operation of the financial transaction system 11 involves operation of a number of transactional processes available to a customer 19 at the electronic kiosk 23 and a number of background monitoring, tracking and handling processes as previously described.

The transactional processes include a customer registration process 43, a send money transaction process 45, a receive money transaction process 47, a foreign exchange enquiry process 81, a reconciliation transaction process 84, a problem resolution transaction process 86, a network management transaction process 88 and a network upgrade transaction process 90.

An overview of the main money transfer processes 41 that can be undertaken by a customer 19 using the electronic kiosk 23 to prepare a financial transaction and then involving counter operator staff of the merchant 15 to complete the preparation and process the transaction is shown in Fig. 2 of the drawings. The money transfer processes 41 basically involve three separate processes that can be performed by the customer at the kiosk, namely the customer registration process 43, the send money transaction process 45 and the receive money transaction process 47. Each of these discrete processes will be described in more detail later, however, as shown in Fig. 2, a customer 19 must first complete the customer registration process 43 before he or she can invoke either the send money transaction money process 45 or the receive money transaction process 47.

Once a customer 19 completes registration and then completes either the send money transaction process 45 or the receive money transaction process 47 at the kiosk 23 for preparation of a financial transaction, the printer 24 produces the barcode voucher 31 in relation to the particular transaction being performed by the customer to complete the first preparatory stage of performing the financial transaction. The customer is then required to take the barcode voucher 31 to the service counter operator 15 and the operator commences the second preparatory stage of the transaction using the services of the facilitator device 25 at step 49.

The counter operator 15 on being handed the barcode voucher 31 is required to process it by using the facilitator device 25 and scanner 27. The counter operator is required to scan the barcode voucher using the scanner 27 and is then prompted by operator instructions displayed on the facilitator device 25 that have been downloaded by the facilitator device from the governing host 21 to undertake the various predetermined steps that need to be completed in order to complete and finally process the transaction.

More specifically, the facilitator device 25 invokes the facilitator process to determine from the barcode voucher 31 whether the transaction is a send money transfer or a receive money transfer at step 51 and indicates such to the counter operator. In the event that it is a send money transfer that needs to be performed, the counter operator is prompted by the facilitator device 25 to undertake the following processes with the customer 19, the counter operator confirming or cancelling the step using the okay or cancel buttons (not shown) provided on the facilitator device 25 to progress through the transaction process before completing and submitting it to the financial service provider. The counter operator:

- verifies the customer identity at step 53;
- receives payment from the customer for the send money transaction at step 55;
- confirms the payment transaction to the financial service provider using the facilitator device 25 at step 57; and
- determines whether the transaction was successful or not at step 59.

If the transaction was successful, then the facilitator device 25 prints out a receipt 33 at the printer 29 and the counter operator staff member 15 provides the receipt 33 to the customer 19 at step 61. The transaction is completed by the facilitator device 25 using the POS transaction key 34 to record the transaction at the merchant POS terminal 17. This completes the send money transaction indicated at 63.

In the present embodiment, the operation of the facilitator device 25 is directly integrated into the merchant POS terminal 17 to communicate with the financial service provider by using a POS API 58. In this manner, the POS transaction key 34, on being generated by the facilitator device 25 is electronically transmitted to the POS terminal 17 by the POS API 58 for recording and completion of the transaction with the financial service provider.

In other embodiments where the merchant does not have a POS API 58 integrating the operation of the facilitator device 25 with the POS terminal 17, the facilitator device prints the POS transaction key 34 for the counter operator staff member 15, and the counter operator staff member enters the POS transaction key into the POS terminal 17 to record and complete the transaction.

If the transaction is not successful, then the counter operator staff member is prompted by the facilitator device 25 as to whether to re-try the transaction at step 65. If the counter operator staff member presses an OK button provided on the facilitator device, then the facilitator device 25 returns to the confirmation of the payment transaction step 57 and continues as before. If the counter operator staff member presses a CANCEL button provided on the facilitator device, the facilitator device 25 steps to complete the send money transaction attempt at 63.

The payment transaction step 57 is invoked by the counter operator staff member pressing the OK button. This causes the facilitator device 25 to invoke an internal process to communicate with the governing host 21, which communicates with an FSP provider 50. It should be appreciated that other merchants may use alternative POS interface services using different POS API's with which the internal process of the facilitator device 25 will communicate.

In the event that the transaction is a receive money transfer that needs to be performed after step 51, the counter operator staff member 15 is prompted by the facilitator device 25 to undertake the following processes with the customer 19. The counter operator staff member:

- verifies the customer identity at step 67;
- confirms the receive money transaction using the facilitator device 25 communicating with the particular money transfer provider of the customer at step 69; and
- determines whether the transaction was successful or not at step 71.

If the transaction was successful, then the facilitator device 25 prompts the counter operator staff member to indicate whether the funds are to be a cash payment to the customer or a prepaid credit card payment, or a combination of both at step 73.

From selecting the particular option, the facilitator device 25 advances to printing a payment transaction receipt 33 at the printer 29 for the customer and a POS transaction key 34 at step 75. The counter operator staff member completes the transaction by entering the POS transaction key 34 on the POS device 17. This step is required if the merchant has not implemented the POS API 58. This completes the receive money transaction as indicated at 77.

If the transaction is not successful then the counter operator staff member is prompted by the facilitator device 25 as to whether to retry the transaction at step 79. If the counter operator staff member presses the OK button, the facilitator device 25 returns to the confirmation of the receive transaction step 69 and continues as before. If the counter operator staff member presses the CANCEL button, the facilitator device 25 steps to complete the transaction at 77.

An important effect of the predetermined steps provided by the operator instructions that prompt the counter operator during the second preparatory stage of the transaction, is that they have been distilled down to their simplest form to allow the merchant to comply with the applicable KYC policy, after the financial transaction system 11 has attended to the bulk of compliance requirements at the kiosk 23 during the first preparatory stage. Moreover, these steps are designed to

resolve that the person who the counter operator is attending to, is in fact the person who is standing in front of them and the person possessing the ID number that was entered on the kiosk. This is executed by the counter operator being prompted by the displayed operator instructions to:

(i) take the photographic identification provided to them by the customer:
(ii) compare the photo on the identification with the person standing before them; and then
(iii) check that the identification number and date of birth displayed on the facilitator device matches the identification number and date of birth provided on the photographic identification.

The customer registration process 43 and the foreign exchange enquiry process 81 can be invoked at the electronic kiosk 23 by a customer 19 preliminary to the customer performing the send money transaction process 45. In the case of the customer registration process 43 this would always be invoked at the outset by a first time user of the kiosk before they are able to invoke the send money transaction process 45.

The customer registration process 43 and the foreign exchange enquiry process 81 will be described in more detail later, however the general process steps involved for both when invoked in a preliminary manner relative to invoking the send money transaction process 45 are shown in Figure 3 of the drawings.

Before any transactional activity is undertaken by a customer 19 at the kiosk 23, the kiosk always prompts the customer to select a language in which they are familiar in order to proceed with the transaction. The customer 19 selects their own language at 82 and all screens then come up in their own language. Terms and conditions and product disclosure statements are then presented to the customer in their own language before proceeding with invoking the customer registration process 43 or foreign exchange enquiry process 81.

On the customer 19 invoking the customer registration process 43, the customer is required to complete registration details at step 83, and the electronic kiosk 23 operates the printer 24 to print a registration receipt at step 85. The customer is then prompted at 87 as to whether they wish to send money now or end the

process. If the customer presses the OK button, the electronic kiosk advances to invoking the send money transaction process 45 as shown. Alternatively, if the customer presses the CANCEL button, the electronic kiosk 23 advances to complete the registration process at 89.

With the foreign exchange enquiry process 81 being invoked by a customer 19, the electronic kiosk 23 advances to requesting the customer to specify the amount, the receiving country and receiving currencies for the enquiry at 91. On providing this information, the money transfer provider enquiry is initiated at 93 and presents the customer with a response to the enquiry at 95. The kiosk 23 prompts the customer as to whether they wish to conduct a new enquiry at 101. If the customer answers in the affirmative by pressing the OK button, the program returns to prompting the customer for the amount and currency at step 91. Alternatively, if the customer responds to the enquiry 101 in the negative by pressing the CANCEL button, the program advances to complete the enquiry stage at 103.

As is mandatory with all financial systems, the financial transaction system 11 is able to reconcile all transactions made at the electronic kiosk 23 and which have been transacted over the counter by operation of the reconciliation transaction process 84. This is shown in more detail at Figure 4 of the drawings and is performed automatically on a daily basis in response to all send money transactions 45 which comprise all payments received from customers by the merchant during the last 24 hours or over a prescribed period of time and all receive money transactions 47 which comprise all payments made to customers by the merchant during the same time. The reconciliation process involves reporting functions performed by the FSP 50 at 105, the POS API 58 of the merchant POS terminal at 107, and the governing host 21 at 109. These respective reports are collated at 111 on a daily basis and reconciled to determine whether they balance at 113. If the reports do balance, a reconciliation report is issued at 115 and a financial settlement between the various service providers is performed at 117. The reconciliation transaction process is then completed at 119. In the event that the reconciliation results in the reports not balancing at 113, then the process steps to investigating and identifying the problem source at 121

and returns to performing the daily reconciliation process 111 again on rectifying the problem.

Now describing the send money transaction process 45 in more detail, reference is made to Figure 5 of the drawings. Although not shown in Fig 5, as described in relation to the customer registration process 43 and the foreign exchange enquiry process 81, the kiosk 23 prompts the customer to select their own language in which to proceed with the transaction. On selecting the desired language, all screens then display in the selected language.

As shown, the send money transaction process 45 on being invoked by the customer selecting the send money option at the kiosk at step 123, prompts the customer for existing registration identification at 125 and advances to receiving either an affirmative or negative response by the customer at 127. If the customer responds by pressing the CANCEL button indicating that they do not have the registration ID, then the process steps to invoking the customer registration process 43. Alternatively, if the customer affirms that they have their registration ID, the program steps to the customer entering their registration ID at 129 and the system ascertaining whether the registration ID is valid at 131. If it is not valid, the program returns to prompting the customer again for their existing registration ID at 125. Alternatively, if the system determines that the registration ID is valid, the program steps to prompting the customer to enter details of the send money request at 133. All of these steps are representative of activity at the kiosk.

On the customer 19 entering their details at 133, the kiosk 23 communicates with the governing host 21 to conduct fraud checking processes 135 and proceeds with the first preparatory stage of the transaction depending upon whether the host system advises that the transaction is to be validated or not at 137. If not, the program returns to prompting the customer to enter details of the send money request again at 133, whereby the process for validating the transaction is repeated. If the host system validates the transaction, then the program advances to the electronic kiosk 23 printing the send money barcode voucher 31 at the printer 24 containing the transaction key at step 139 and the customer is prompted to present the voucher to counter operator staff.

On the customer presenting the barcode voucher 31 to the merchant's counter operator at 141, the operator proceeds with the second preparatory stage of the transaction by logging into the facilitator device 25 at 142 and the facilitator device downloading a set of operator instructions from the governing host 21, which are followed. These include instructing the operator to validate the identification documents provided by the customer and collect payment from the customer at 143.

The operator must be registered with the financial transaction system 11 in order to operate the facilitator device 25. The governing host 21 retains a log of unique identifier codes of all counter operators who are authorised by the merchant to operate the facilitator device 25. The log also provides an indication as to whether the counter operator has successfully completed a training course on how to operate the facilitator device and apply the business rules of the merchant to comply with KYC policy requirements at the counter when dealing with a customer. Unless the operator identity on the log has been asserted to indicate that the operator has been appropriately trained, the facilitator device 25 will not permit the operator to operate the facilitator device 25.

On the operator logging in to the facilitator device 25 with their unique identifier at 142, the facilitator device checks with the governing host 21 whether the operator appears on the log and is clear to operate the facilitator device having passed training and process a financial transaction. If clear, the governing host 21 downloads the appropriate operator instructions. The operator then initiates the send money request by scanning the barcode voucher at step 145 using the facilitator device 25. The operator follows the operator instructions by completing the identity check and collecting the tendered amount, then confirms that these checks have been completed on the facilitator device. The governing host 21 then receives the voucher request at 147. The host system 21 consolidates the voucher information with the customer registration and send money request data entered by the customer 19 at the kiosk 23 at 149, whist simultaneously the governing host performs fraud checking against the compliance rules set for the merchant transactions at 151 and ascertains whether the voucher request is valid at 153. If so, the governing host 21 completes the transaction using the FSP

interface 50 at 155. If the voucher request is not valid, the governing host rejects the voucher request at 157 and steps to sending a reject message to the facilitator device 25 at 159.

If the send money request proceeds successfully at 161 the FSP interface 50 provides a money transfer reference number to the governing host 21 which sends a receipt to the facilitator device 25 in respect of the send money transaction at 163. If the send money request does not proceed successfully, the FSP interface 50 directs the governing host to send a reject message to the facilitator device 25 at 159. The facilitator device 25 at step 165 indicates to the counter operator to provide the receipt to the customer and process the sale at the merchant POS 17 using the POS transaction key 34 at 167. If the transaction was successful at 169, process is completed at 171. If the transaction was not successful at 169, the counter operator is prompted as to whether they wish to retry the transaction at 173. If it is decided not to retry the transaction, then the process is completed at 171. Alternatively, if it is decided to retry the transaction, the counter operator proceeds to initiate a send money request once more at 145 by scanning the barcode voucher 31 using the scanner 27 of the facilitator device 25 and the process is repeated once more.

The receive money transaction process 47 is shown in detail at Figure 6 of the drawings and is invoked by the customer selecting the receive money option provided at the electronic kiosk at 175. Before doing so, as described in relation to the customer registration process 43, the foreign exchange enquiry process 81 and the send money option at 45, the kiosk 23 prompts the customer to select their own language in which to proceed with the transaction. On selecting the desired language, all screens then display in the selected language.

As in the send money process 45, the customer is prompted for their existing identification for using the system at 177. If the customer does not have their registration identification at 179, the customer is prompted to enter details for the receive money process at 181. In the event that the customer does have their registration ID at 179, the customer enters their registration details at 183 and the system proceeds with checking whether the registration ID is valid or not at 185. If the registration ID is not valid, the program returns to prompting the customer

for their existing registration identification once more at 177 and proceeds as before. If the registration ID is valid at 185, or if the customer is prompted for entering details for receiving money at 181, the program steps to the customer entering details of the receive money request at 187. The governing host is then invoked to perform fraud checking in accordance with the rules governing the transactions of the particular merchant at 189. The governing host 21 ascertains whether the transaction is valid and informs the kiosk as to whether it is appropriate to proceed with the first preparatory stage of the transaction at 191. If the transaction is not validated at this stage, the program returns to requiring the customer to enter the details of the receive money request again at 187.

If the transaction is validated at 191, the barcode voucher 31 is printed by the printer 24 at the kiosk 23 and received by the customer at 193. The customer then presents the voucher to the counter operator of the merchant at 195 to commence the second preparatory stage of the transaction. As described in the send money process, the counter operator logs in to the facilitator device with their unique identifier at 196 and upon being cleared by the governing host 21, the operator instructions are downloaded from the governing host to the facilitator device 25, whereupon the counter operator validates the identification documents provided by the customer at 197. The counter operator staff member then initiates the receive money request by scanning the voucher 31 at the scanner 27 of the facilitator device 25 at step 199. The governing host 21 then receives the voucher request at 201. The governing host 21 consolidates the voucher information with the customer registration and receive money request data entered by the customer 19 at the kiosk 23 at 203. The governing host then performs fraud checking against the business rules applying to transactions of the particular merchant at 205 and determines whether the voucher request is valid or not at 207. If the voucher request is valid, the governing host 21 completes the second preparatory stage of the transaction by transmitting the receive money request to the FSP using the FSP interface 50 at 209. If it is not valid, the governing host rejects the voucher request at 211 and sends a reject message to the facilitator device 25 at 213. Similarly, if the FSP interface 50 determines from the FSP that the receive money request is not successful at 215, the governing host similarly is prompted at 213 to send a reject message to the facilitator device 25.

If the receive money request at 215 is successful, then the governing host sends a receipt and a POS transaction key to the facilitator device 25 at 217. If the transaction is successful at step 221, the counter operator staff member is prompted to provide payment to the customer at step 223 and completes the process shown in the overview 41 at Figure 2 of the drawings, at which stage the entire transaction process is completed at 225. On the other hand, if the transaction is not successful, then the counter operator staff member is prompted to retry the transaction at 227. If the counter operator staff member chooses not to retry the transaction, then the process is completed at step 225, or alternatively if the counter operator staff member decides to retry the transaction, then the counter operator staff member initiates the receive money request and scans the barcode voucher 31 once more at step 199, repeating the aforementioned process steps again.

Now describing the registration transaction process 43 in more detail, reference is made to Figure 7 of the drawings. According to this process, after selecting the requisite language at 82, the customer selects the registration option at the electronic kiosk at step 229, which then prompts the customer to enter full registration details at 231. Typical registration details that are prompted for entry are shown below.

Customer Registration:

First name	mandatory entry
Middle	optional
Last name	mandatory entry
Address	mandatory entry
Town	mandatory entry
Country	mandatory entry. Validated from dropdown list
Postcode	mandatory if country is USA or Australia
State	mandatory if country is USA or Australia. Validated via dropdown list
Occupation	mandatory entry
Birthdate	mandatory entry, checked to ensure a valid date
Birth country	mandatory entry. Validated from dropdown list
Photo ID type	mandatory entry, must be Driver's Licence or Passport
Photo ID No.	mandatory entry. Cannot already be on the database for this person (to stop duplicate registrations)
Mobile phone No.	mandatory entry

email address	optional

The governing host 21 receives the registration request detail at 233 and processes the request at 235. The kiosk 23 then invokes the printer 24 to print the registration voucher, which is received by the customer at 237. The customer is then prompted to invoke the send money transaction process at 239. Depending upon the response of the customer at 241, the send money transaction process 45 is invoked if the customer responds affirmatively, or alternatively the process is completed at 243 if the customer does not wish to proceed with sending money.

If the customer is going to send money by invoking the send money transaction process 239, the customer will be prompted to enter the recipient details at the kiosk 23. Typical recipient details that are prompted for entry are shown below.

Recipient detail entry:

First name	mandatory entry
Middle	optional
Last name	mandatory entry
2nd Last name	optional
Address	mandatory entry
Town	mandatory entry
Country	mandatory entry. Validated from dropdown list
Postcode	Required if country is USA or Australia.
State	Required if country is USA or Australia. Validated via dropdown list

The foreign exchange enquiry process 81 is shown in detail at Figure 8 of the drawings, in response to it being invoked as part of the process described with respect to Figure 3 of the drawings after the customer selects the requisite language to conduct the enquiry in at 82. It commences with the customer selecting the enquiry option provided at the kiosk at step 245. The kiosk then prompts the customer to enter the amount and the receive country and receive currencies at 247. On entering the same, the governing system host 21 receives the enquiry request at 249 and proceeds to process same at 251 by communicating with the FSP 50 to retrieve the relevant information as sought by the enquiry at 253.

On receiving this information, the electronic kiosk 23 displays the enquiry send and receive values at 255 and the customer is prompted as to whether they wish to make a new enquiry request at 261. If the customer responds in the affirmative to making a new enquiry request, the kiosk prompts the customer to enter the send and receive currency amounts at step 247 again, and the process is repeated. If the customer responds declining the new enquiry request, the process is completed at step 263.

The problem resolution transaction process 86 is shown in Figure 9 of the drawings and arises when the customer has a problem that is brought to the attention of a counter operator staff member 15, as indicated at step 265. Depending upon whether the problem occurs in the store or not, as indicated at step 267, there are one of two ways of proceeding. If the problem occurs in the store, the counter operator staff member provides details to a helpdesk operator of the merchant at 269 where the store is one of a chain of stores managed by the merchant. If the problem occurs outside of the store, the customer receipt provided by the electronic kiosk 23 provides helpdesk contact details at 271. In either case, the customer ultimately contacts the helpdesk operator of the merchant at 273. The merchant's helpdesk operator then follows a prescribed set of resolution scripts provided to them by the governing host at 275 to allow the merchant to assist the customer and attempt to resolve the problem. If the problem is resolved at 277, then the process is completed at 279. If the problem is not resolved at 277, the helpdesk operator for the merchant contacts the helpdesk operation 30 of the governing host 21 at 281. The governing host helpdesk operator 30 then records the problem and customer details at 283 and makes contact with the customer at 285 to help resolve the problem at 287. Once the problem is solved the helpdesk operator 30 then confirms resolution of the problem with the helpdesk operator of the merchant at 289, thereby completing the process at 279.

If the problem is sourced with the store of the merchant as shown at 291 as opposed to a customer, the merchant store firstly contacts the helpdesk operator of the merchant at 293 and the helpdesk operator of the merchant follows the resolution scripts provided by the governing host 21 at 275. Thereafter, the

problem resolution transaction process is performed as before, being escalated to the governing host helpdesk provider 30 at the appropriate stage if necessary.

A network management transaction process 88 is shown in detail in Figure 10 of the drawings and involves a local kiosk help monitoring process 295 and a remote kiosk help monitoring process 297.

The local kiosk help monitoring process 295 involves a local kiosk monitoring service detecting a problem requiring action at 299. In response to same, the kiosk sends an alert to the governing host 21 at 301. Depending upon whether the alert is received by the governing host 21 at 303 after a prescribed time, the kiosk sets a restart time and retries the process at 305. If the restart time has not yet expired at 307, another alert is sent to the kiosk service at 301 and the process repeated. If the restart timer has expired at 307, then the electronic kiosk 23 is restarted at 308 in an attempt to invoke communications with the governing host 21 once more.

If the alert is received by the governing host 21 at 303, the kiosk service of the governing host 21 analyses the alert at 309 and automatically invokes a remote fix of the problem if possible at 311. If it is not possible to remotely fix the problem, the issue is escalated to on call support services at 313. On the other hand, if it is possible to fix the problem automatically, the kiosk service sends notification of the fix via the governing host to the electronic kiosk 23 at 315, and the kiosk applies the fix and sends an acknowledgement to the governing host 21 at 317. If the kiosk ascertains that the fix is successful at 319, then the process reverts to the local kiosk helpline at step 295 once more. If the fix is not successful at 319, the kiosk ascertains whether multiple fix attempts have been made at 321. If not, then an alert is sent to the kiosk service at step 301 and the process repeated. If there have been multiple fix attempts, the issue is escalated to on call support at 313.

With the remote kiosk help monitoring process at 297, a remote kiosk monitoring service is invoked to detect whether a problem arises requiring action at 323. If so, the kiosk service analyses the alert at 325 and automates a remote fix if possible at 327. If it is not possible to remotely fix the problem automatically, the issue is escalated to on call support at 313. On the other hand, if it is possible to

remotely fix the problem, then the kiosk service sends the fix to the electronic kiosk by way of the governing host 21 at 329. The kiosk, on receiving the fix, applies it and sends an acknowledgement to the kiosk service of the governing host 21 at 331. If the fix is successful at 333, then the remote kiosk help monitoring process 297 is invoked again for normal remote monitoring. If the fix is not successful at 333, then it is determined whether multiple fix attempts have been undertaken at 335. If they have, then the issue is escalated to on call support at 313. If not, then the kiosk service is invoked to send a fix to the kiosk at 329 once more.

The network upgrade transaction process 90 is shown in Figure 11 of the drawings. The network upgrade transaction process 90 involves kiosk software management and upgrade performed by the governing host 21, as indicated at step 337. When invoked, the remote kiosk update service initiates a software/product upgrade at 339 and sends required changes to the kiosk at 341. It then sets a timer at the governing host for receiving an acknowledgement from the electronic kiosk 23 that the changes have been received by the kiosk at step 343. The process then ascertains whether the timer has expired at 345, and if so, escalates the issue to on call support at 347. If the timer has not expired and an acknowledgement is received from the kiosk at 349, the kiosk service records that the change has been made to the kiosk at 351 and the process is completed at 353. On the kiosk receiving the software/product change it applies same at 355 and sends an acknowledgement to the kiosk service at the governing host 21 at 357. It then proceeds to check whether an acknowledgement has been received by the kiosk service at 359. If so the kiosk service records the change made to the kiosk at 351 and completes the process at 353. If the acknowledgement is not received, the kiosk sets a kiosk restart timer and retries sending the acknowledgement to the kiosk service at 361. If the restart timer has not expired then the kiosk proceeds with sending the acknowledgement to the kiosk service at 357 and the process is repeated. If the restart timer has expired at 363, it proceeds to restart the kiosk and attempt to establish communications with the governing host 21 once more at 365.

Now describing the background monitoring, tracking and handling processes in more detail, as shown in Fig 12, the compliance monitoring process and fraud checking process are effectively run by the same compliance/fraud monitoring engine 401 located on the governing host 21. The compliance/fraud monitoring engine 401 includes a trigger setting process 403 to allow one or more compliance triggers to be defined and configured either remotely or locally of the governing host 21 by the governing host administrator/manager 20 for a merchant in respect of financial transactions to form the compliance framework of the merchant, which is downloaded and processed by the kiosk 23, to apply the business rules of the merchant during the preparatory stages of financial transactions prepared at the kiosk. In the present embodiment, parameters can be set for compliance triggers limiting the time period within which transactions may be processed, limiting the volume of transactions that can be performed and/or limiting the value of transactions. These can be based on a particular merchant, customer, store or group of stores and help define the compliance framework of the merchant.

Once the limits of these compliance triggers are set, they are stored in the database 22 of the governing host and a transaction examining process 405 is invoked to ensure compliance with the business rules of a the merchant and to activate any fraud alerts in response to any and all transactional activity at the kiosk 23. Each customer registration process 43, send money transaction process 45, receive money transaction process 47, foreign exchange enquiry process 81, problem resolution transaction process 86, network management transaction process 88 and network upgrade transaction process 90 of the transactional processes that are performed for a customer at the kiosk 23 are examined. The transaction examining process 405 examines each individual transaction to ensure compliance and ascertain whether a compliance trigger limit that could suggest money laundering, terrorism financing or fraudulent activity has been breached and if so, invoke a prescribed contingency process, depending upon the particular compliance trigger that has been breached.

In the present embodiment, the prescribed contingency processes include a stop process 407, the alert process 409 previously described and a compliance report process 411.

The stop process 407 is programmed to stop any further transacting occurring after a set limit of a compliance trigger is reached.

The alert process 409 is programmed to launch a manual investigation process when a particular predefined compliance trigger has stopped a transaction. The alert process 409 initiates the sending of an email or text message to a defined person or group of people who investigate and examine the transaction for suspicious behaviour that may indicate an attempt at money laundering or fraud.

Some examples of the use of set limits, alerts and triggering events are as follows:

- a customer send amount may be set to be not more than $2,500. Some countries may have lower limits imposed by law or a merchant may set a limit lower in countries where higher risks of money laundering, terrorism financing or fraud have been identified. For example in Nigeria or Ghana, the maximum send amount could be set at $900.
- a customer limit can be set to trigger when the end customer sends $2,000 in any three hour period, $9,000 in any one day across all stores, or 10 transactions in a day. This may be set to meet a regulatory requirement.
- An individual store can have a daily limit triggered when the store has received $10,000 in total in a given day and may also have a three hourly limit of $5,000. All stores in a particular region can have a limit of $100,000 in any day. This manages the credit risk on the merchant's store as transactions will not be allowed when these limits are hit and is part of the merchant's risk policy which is also part of their compliance program.
- Transactions that originate in another region and are sent to that region may indicate staff fraud. An alert is launched and a manual process used to follow up to ensure cash has been received.

- Transactions sent to Nigeria may indicate part of a scam. An alert can be sent and a manual process used to investigate whether scam potential exists for reporting to regulators.

The compliance report process 411 is compiled by the governing host 21 based on particular compliance triggers that are defined in the merchant's compliance program and is invoked to compile a compliance report at regular periods defined in the compliance program, e.g. daily, weekly and monthly. These compliance reports are reviewed by a compliance officer or their agent for suspicious activity and may be necessary to send to a regulator as part of a regulator report.

For example, a compliance report may be produced daily in respect of all transactions processed by a merchant across the merchant network for the previous 24 hour period. The compliance report is reviewed for any unusual, suspicious or fraudulent activity. For example, the following exceptions are reported and transaction details shown:

Agent Location activity	Agent Locations with 3 or more transactions where each transaction is $800 or more
Sender activity	Sender name occurs more than once for an Agent Location with 3 or more transactions where each transaction is $800 or more
Recipient activity	Recipient name occurs more than once for an Agent Location with 3 or more transactions where each transaction is $800 or more
Sender photo ID activity	Sender photo id occurs more than once for an Agent Location with 3 or more transactions where each transaction is $800 or more
Sender DOB activity	Sender's date-of-birth (**DOB**) occurs more than once for an Agent Location with 3 or more transactions where each transaction is $800 or more
Sender address activity	Sender address Line 1 occurs more than once for an Agent Location with 3 or more transactions where each transaction is $800 or more
Suspicious ID number	Transaction details for a customer with a suspicious Photo ID Number. The parameters for suspicious ID number are less than 5 characters or have 4 successive alpha characters. Where the ID is suspicious, the Cullinan System will replace it with *INVALID ID* code so that the customer must correct it before transacting again.

In the case of weekly transaction monitoring, a compliance report may be produced in respect of all transactions processed by a merchant across the merchant network for the previous 7 days. The compliance report is reviewed for

any unusual, suspicious or fraudulent activity. For example, the following exceptions are reported and transaction details shown:

Sender activity	Sender name and DOB combined > 7 transactions and value is over $2,500. Sender is placed on ECDD.
	Sender name and DOB combined > $20,000. Compliance Officer will submit a SMR for each of these occurrences.
	Sender address > 7 transactions and value is over $2,500. Sender address is placed on ECDD.
	Sender address > $20,000. Compliance Officer will submit a SMR for each of these occurrences.
	Listing of transactions for send amount > $800 and DOB < 01-01-1950
Recipient activity	Recipient name and recipient town combined > 7 transactions and value is over $2,500. Recipient is placed on ECDD.
	Recipient name and recipient town combined > $20,000. Compliance Officer will submit a SMR for each of these occurrences.
	Recipient address > 7 transactions and value is over $2,500.. Recipient address is placed on ECDD.
	Recipient address > $20,000. Compliance Officer will submit a SMR for each of these occurrences.
Receiver activity	Receiver name and DOB combined > 7 transactions and value is over $2,500. Receiver is placed on ECDD.
	Receiver name and DOB combined > $20,000. Compliance Officer will submit a SMR for each of these occurrences.
Corridor activity	Listing of transactions for send amount > $900 and recipient country is Australia
	Listing of transactions for send amount > $850 and recipient country is Nigeria or Ghana

In the case of monthly transaction monitoring, a compliance report may be produced in respect of all transactions processed by a merchant across the merchant network for the previous month. The compliance report is reviewed for any unusual, suspicious or fraudulent activity. For example, the following exceptions are reported and transaction details shown:

Sender activity	Sender name and DOB combined > 20 transactions and value is over $9.000. Sender is placed on ECDD.
	Sender name and DOB combined > $50,000. Compliance Officer will submit a SMR for each of these occurrences.
	Sender address > 20 transactions and value is over $9.000. Sender address is placed on ECDD.
	Sender address > $50,000. Compliance Officer will submit a SMR for each of these occurrences.
	Listing of transactions for send amount > $800 and DOB < 01-01-1950
Recipient activity	Recipient name and recipient town combined > 20 transactions and value is over $9.000. Recipient is placed on ECDD.
	Recipient name and recipient town combined > $50,000. Compliance Officer will submit a SMR for each of these occurrences.
	Recipient address > 20 transactions and value is over $9.000. Recipient address is placed on ECDD.
	Recipient address > $50,000. Compliance Officer will submit a SMR for each of these occurrences.
Receiver activity	Receiver name and DOB combined > 20 transactions and value is over $9.000. Receiver is placed on ECDD.
	Receiver name and DOB combined > $50,000. Compliance Officer will submit a SMR for each of these occurrences.
Corridor activity	Listing of transactions for send amount > $900 and recipient country is Australia
	Listing of transactions for send amount > $850 and recipient country is Nigeria or Ghana
	Exception report of all corridors that have increased volume of transactions > 30% over the prior month
Agent Location activity	Exception report of all Agent Locations that have increased volume of transactions > 30% over the prior month

If the compliance officer regards a customer's or merchant's behaviours as suspicious, then the compliance officer may file a regulator report. Regulator reports could include a suspicious matter filed in a compliance report and may be filed with the regulator, and included in a report to police or an FTP.

As a consequence of this, a compliance officer may place a customer or merchant on enhanced customer due diligence (ECDD). If a customer is placed on ECDD, the transactions are then individually reviewed at a period defined in the compliance program by the compliance officer.

As previously described, the transaction examining process 405 is performed each time that a customer enters details at the electronic kiosk 23. Thus if the

business rules of the merchant, as determined by the limits set by the trigger setting process 403, are not followed, or mandatory information is not provided, the customer cannot complete the registration or transaction. This means that a correctly completed form must be entered by the customer in accordance with the compliance program before the customer reaches the counter.

The sales tracking process 413, as previously described, is implemented on the governing host 21 and records the merchant location from which a quote was initiated from and the contents of that quote, e.g. destination country and whether the transaction was concluded. This data is then compared to other stores to highlight any material differences. If the ratio of quotes to transactions to a particular country varies materially across stores, it is a lead indicator that pricing needs to be adjusted.

The customer tracking process 415, as previously described, is also implemented on the governing host 21 and involves rules that are set to identify particular customers who subscribe to the service and are performing transactions differently to their previous behaviour. Details of these customers are loaded into the governing host 21 and some prescriptive action is undertaken. For example, the customer tracking process runs a program to calculate the number of times on average each subscribing customer transacted over a predetermined period of time, e.g. an average of X times in Y months, and then calculates the number of transactions that occurred in the last month. If they have transacted less than Y/X then the governing host 21 can send an email coupon to those customers.

The coupon can then be redeemed at a facilitator device and a report produced on whether the coupon has been redeemed.

The generalised products and services handling infrastructure 417 is shown at Figs 13 and 14 and allows for third party products and services to be added, modified and transacted on the electronic kiosk 23 and facilitator device 25 cost effectively with minimal intervention by the host administrator/manager 20 and merchant. Consequently, the merchant is able to implement third party products and services on the kiosk 23 and reconcile sales involving those products and services via the facilitator device 25 at point-of-sale and complete financial transactions using the POS terminal 17 as a standard product or service item.

The business process flow 418 is shown in Fig 13 and commences with displaying the third party service interface on the kiosk 23 at step 419, as an option for the customer 19 to select. On the customer 19 completing a request via the third party service interface at step 421, the third party service provider 422 returns a Request Number to the kiosk 23 at step 423 and the kiosk prints out the Request Number in the format of a barcode voucher 425 using the kiosk printer 24. The customer 19 then takes the voucher 425 to the counter of the merchant's store for processing at step 427 and the store operator 15 scans the voucher 425 using the scanner 27 of the facilitator device 25 at step 429. The facilitator device 25 then makes a request to the governing host 21 for operator instructions on how to process the third party transaction at step 431 and on obtaining these instructions, returns them for display to the operator 19 at step 433. The facilitator device 25 on relevant prompting and complying with the business rules of the merchant attends to requesting the financial transaction using the POS API 58 with the third party service provider 422 via the POS terminal 17 at step 435 and on the governing host 21 verifying and the third party service provider 422 validating the transaction, the financial transaction is completed at step 437.

As shown in Fig 14, the various components of the financial transaction system 11 interact with the third party service provider 422 and customer 19 to create the infrastructure 417. Essentially, the electronic kiosk 23 has an application that is capable of launching a third party service through a web interface. The interface lists third party services and the URL's that the application uses to connect to them in a set of third party service definitions 439 stored in the database 22 of the governing host 21. In this manner, a third party service can be selected by a customer on the electronic kiosk 23, which will be invoked using the defined URL with an Agent ID that identifies the location of the electronic kiosk 23.

In this interaction, the governing host 21 is placed to initiate all requests via the electronic kiosk 23 from a customer 19 accessing a third party service provider 422 via the displayed third party service interface. Consequently, the third party service provider 422 only provides a response to requests so initiated, permitting the governing host 21 to undertake compliance and fraud checking tasks. Furthermore, the governing host 21 only initiates requests to third party service

providers 422 with whom it has defined an interaction as listed. These definitions are established in conjunction with a defined third party service provider 422 via a third party service administration interface 441.

The third party service is configured to perform all of its activities within the confines of the web browser interface and complete its function in one of three ways:

(i) Exit with the Request Number being supplied to the kiosk user interface for display and/or printing;
(ii) Exit without a Request Number being issued: or
(iii) Suffer a forced closure by the kiosk user interface due to a time-out expiry.

The Request Number only has relevance to the third party service provider and in the present embodiment contains an 8-digit product code, although in other embodiments it can be anything up to a 12-digit Voucher Number.

Where possible, the third party service web interface is cached on the electronic kiosk 23. This depends upon the caching rules defined the third party service definition 439 and the implementation by the third party service provider 422.

The database 22 of the governing host 21, as previously described, is specifically designed to store relevant customer interactions with the financial transaction system 11 for marketing, business risk management and compliance purposes.

Another characteristic of the financial transaction system 11 of the specific embodiment is its ability to deliver operator management, administration and training. This characteristic not only has the practical effect of meeting quality assurance requirements in training counter operator staff on the correct use of the financial transaction system, but also can be leveraged to insure the merchant against an infraction by a customer at the merchant's store of AML/CLF legislation or fraudulent activity despite full compliance of the counter operator with the business rules of the merchant adhering to KYC policy requirements. Furthermore, the financial transaction system 11 can provide important proof of compliance as a defence under AML/CLF legislation to non-compliance with KYC policy and provide an auditable trail that could constitute evidence to prove illegal behaviour of a customer leading to their conviction.

As shown in Fig 15, the financial transaction system 11 includes a training setting process 445 that has options for defining merchant store administrators, store counter operators and counter operator training settings.

With defining store administrators, the training setting process 445 is programmed to define a new store administrator at 447, which firstly entails defining the store of the merchant that the administrator is allowed to administer at 449 and then assigning the administrator of that store a password at 451. At this stage, a training completed flag for the administrator is automatically set to FALSE at 453. The credentials of the store administrator that have been set up can then be communicated to the administrator at 455. Once training of the administrator is completed, the training setting process 445 can be invoked to change the training completed flag of the administrator to TRUE.

The store administrator, once asserted to be trained, can then define new store counter operator staff at 457 with a unique identifier. The definition of the new counter operator involves the store number that the administrator has permission rights to, being assigned by default to the counter operator at 459. Similarly, at this stage, a training completed flag for the defined counter operator is automatically set to FALSE at 461 and a password for the counter operator is optionally defined at 463.

The mandatory training program for counter operator staff is commenced at 465 and the counter operator's unique identifier that was assigned as part of the operator's definition at 457, entered at 467. When the mandatory training program is completed at 469, the training completed flag for the counter operator is then set to TRUE at 471. At this stage, the counter operator is eligible to process transactions at point of sale for the merchant at the defined store, as indicated at 473.

The relevant information concerning the administrator and counter operator identities, passwords and training status is stored on the database 22 of the governing host 21.

As previously mentioned in conjunction with the description of the send money transaction process 45, this information is made use of in verifying the identity of a

counter operator and their ability to use the facilitator device 25 at the POS counter of the merchant's store, according to the status of the training competed flag. It also is used as the trigger when verified by the counter operator to download the operator instructions to the facilitator device 25 providing the compliance framework sourced on the governing host 21 that manages the activities of the counter operator to ensure compliance with the business rules of the merchant during the second preparatory stage of processing a financial transaction with a customer who has completed the first preparatory stage of the transaction at the electronic kiosk 23.

The governing host 21 can then apply an operator stamp listing the unique identifier of the store, the counter operator and whether they have been trained or not, to a log of financial transactions performed using the facilitator device 25 as proof that a trained operator processed any of the logged transactions. This log can then be used as a defence to verify and prove compliance by trained operators in accordance with KYC policy.

It should be noted that the present embodiment provides many advantages over other types of money transfer systems. These include:

1. The ability of the governing host 21 to use pattern analysis in order to analyse transactions for suspicious matters, centrally. If there is a suspicious matter detected, a central compliance officer is alerted who takes action in accordance with the risk and regulator policy. Thus only the compliance officer needs to be highly skilled and trained in this regard, and not the counter operator staff member 15 of the merchant. This means that staff training can be reduced to skilling in "checking the id" of the customer 19 and reporting anything that is visually suspicious to the help desk for investigation.
2. The barcode voucher 31 including a barcode that is a standard point of sale barcode. The counter operator staff member 15 of the merchant processes this on the merchant POS terminal 17 as a normal product. This means that cash is recorded going into the till of the merchant as a normal product and can be reconciled as a normal product, which is not the case for money transfers in the past, where a separate till was required.

3. A language handling facility, where:
    a. A file is stored on the governing host 21 from which languages can be selected by the electronic kiosk 23, so that a kiosk screen saver will display advertising only in those selected languages;
    b. A process is provided for allowing a user of the electronic kiosk 23 to select a language displayed on the kiosk screen, wherein after the terms and conditions of the money transfer will be presented in that language; and
    c. Receipts can be presented in the selected language.
4. A process for identifying lost customers from the governing host database, and then couponing them to encourage them to return.
5. The fraud and compliance checking configurable rules being embedded in the "kiosk - facilitator device - transaction process" to restrict or alert on transactions based on many sets of rules that can be updated regularly as regulator and retailer policies change on behalf of the merchant and allowing the merchant to configure these rules whenever they want to.

It should be appreciated that in the preferred embodiment, these advantages are essentially achieved by the financial transaction system performing the following process:

(a) Receiving data entered by the user;
(b) Presenting the terms and conditions on the kiosk screen in the customers own language (this provides the first part of a legal "offer");
(c) Disclosing the transaction and having it accepted by the customer in their own language on the electronic kiosk, including exchange rate, fees, taxes and receive money transfer network limitations and any other items that require disclosure (this provides the second part of a legal "offer" and full transparency for the consumer);
(d) The consumer accepting the terms and conditions in their own language (providing the legal "acceptance"); and
(e) Validating the entire transaction by the governing host 21 prior to the customer 19 getting to the counter of the merchant to effect the transaction - if there are problems, the consumer can fix the problems at the electronic

kiosk 23 prior to getting to the facilitator device 25, thus ensuring that virtually all transactions go through when the customer gets to the counter.

The above is in contrast to other systems where many transactions are rejected at the counter and the counter operator staff have to have a conversation with the customer at the counter to address and rectify the problem.

It should be appreciated that many other processes are performed by the financial transaction system 11 in order to achieve the functions specifically referred to in the description. The implementation of these processes, given the description of the specific processes referred to above, would be reasonably straightforward to a person skilled in the art and will not be described in further detail. Thus, the scope of the present invention is not limited to the specific embodiment described above and other embodiments or variations of financial systems and processes for performing the same are envisaged and form part of the invention.

MCSLLP

CLAIMS

1. A financial transaction system for preparing parties for a financial transaction to be processed by a financial service provider, including:

a governing host having a database for registering the parties wishing to perform a financial transaction between them using the financial service transfer provider to ultimately process the financial transaction;

a discrete terminal independently accessible by one party of the parties wishing to initiate a financial transaction with another party of the parties and for communicating with the governing host to prepare for the transaction, the discrete terminal having a local transaction process providing for the initial validating and enforcing of business rules governing the transaction with the one of the parties and to generate a transaction key confirming that the initial validating and enforcing has been successful to complete a first stage of the financial transaction and that a second stage of the transaction is authorised by the governing host to proceed;

a facilitator device for completing the second stage of the financial transaction at a point-of-sale terminal of the other of the parties, the facilitator device having a reader to read the transaction key on being supplied with same from the one of the parties and communicating with the governing host to complete the transaction using the facilitator device;

the discrete terminal being located separately and capable of being accessed and operated independently by the one of the parties, offline of any point-of-sale activity involving the point-of-sale terminal and the facilitator device;

the facilitator device including a facilitator process to instruct the other of the parties on those steps required to complete a transaction in a manner that complies with the rules of a regulator of the provision of the financial transaction as well as the business rules of the other of the parties;

wherein the governing host includes a process to enforce compliance requirements dependent on the business rules that need to be complied with by the other of the parties, before submitting the financial transaction for

processing by the financial service provider, in response to communication with the discrete terminal as part of the local transaction process;

and wherein the discrete terminal includes a process to validate or reject the transaction having regard to compliance with the business rules governing the transaction that are required to be performed by the other of the parties in response to being provided with the transaction key.

2. A financial transaction system as claimed in claim 1, wherein the facilitator device is integrated into the point-of-sale terminal.

3. A financial transaction system as claimed in claim 1 or 2, wherein the local transaction process includes a customer registration process, a send money transaction process, a receive money transaction process, or a foreign exchange enquiry process.

4. A financial transaction system as claimed in any one of the preceding claims, wherein the facilitator process includes a discrete facilitator process for prompting the other of the parties to conduct an identity check of the one of the parties and validating the transaction for submitting to the financial service provider only after the other of the parties has verified completion of the identity check.

5. A financial transaction system as claimed in any one of the preceding claims, wherein the discrete terminal and governing host provide for the operation of supplemental transaction processes, including a reconciliation transaction process, a problem resolution transaction process, a network management transaction process and a network upgrade transaction process to facilitate and support the operation of the financial transaction system.

6. A financial transaction system as claimed in any one of the preceding claims, wherein the governing host system includes fraud detection means to analyse patterns of transactions that may be fraudulent or non-compliant and to alert when detecting same.

7. A financial transaction system as claimed in claim 6, wherein the discrete terminal includes a fraud detection process responsive to said fraud detection

MOSLLP

means to validate the initial transaction before authorising the transaction to proceed to the next stage.

8. A financial transaction system as claimed in any one of the preceding claims, wherein the governing host includes a report process for automatically generating reports for submission to the regulator as part of the compliance program of the other of the parties.

9. A financial transaction system as claimed in any one of the preceding claims, wherein the facilitator device includes a discrete facilitator process for creating a record of the financial transaction for submitting to the financial service provider only created after the other of the parties has verified the conduct of the identity checks.

10. A financial transaction system as claimed in any one of the preceding claims, wherein the facilitator device, at the end of some transactions loads a banking card for the one of the parties with sums of money that the one of the parties can then use to withdraw at an automatic teller or other money dispensing machine.

11. A method for preparing for preparing parties for a financial transaction to be processed by a financial service provider including:

registering one of the parties for performing a financial transaction offline from any point-of-sale activity;

receiving a request from a registered party wishing to initiate a particular type of financial transaction with another of the parties offline of any point-of-sale activity involving the other of the parties;

communicating with a governing host to prepare for the transaction using a local transaction process providing for the initial validating and enforcing of business rules that need to be complied with by the other of the parties governing the transaction with the one of the parties;

generating a transaction key on the governing host and the local transaction process validating the transaction;

completing the next stage of the financial transaction by prompting the other of the parties to further validate the transaction in accordance with compliance requirements of the other of the parties on being provided with the transaction key, and submitting the financial transaction with the financial service provider at point-of-sale for processing after communicating with the governing host as appropriate to further validate the transaction.

12. A method for preparing parties for a financial transaction as claimed in claim 11, wherein the step of receiving a request from a registered party occurs locally of the other of the parties but offline of any point-of sale activity involving the parties.

13. A method for preparing parties for a financial transaction as claimed in claim 11 or 12, including delivering point-of-sale material and displaying instructions, terms and conditions to the one of the parties in the their own language, prior to completing the transaction.

14. A method for preparing parties for a financial transaction as claimed in any one of claims 11 to 13, including submitting the financial transaction for processing by the financial service provider only after prompting the other of the parties to conduct identity checks of the one of the parties based on the electronic delivery of instructions to the other of the parties by the governing host.

15. A method for preparing parties for a financial transaction as claimed in any one of claims 11 to 14, including applying the risk and fraud rules of the other of the parties as part of the initial validating and enforcing performed by the local transaction process.

16. A method for preparing parties for a financial transaction as claimed in any one of claims 11 to 15, including the local transaction process receiving alerts of fraudulent or non-compliant transactions from the governing host, analysing the request having regard to same, and alerting when detecting same.

17. A method for preparing parties for a financial transaction as claimed in any one of claims 11 to 16, including automatically generating reports for submission to the regulator as part of the compliance analysis requirements of the other of the parties.

18. A method for preparing parties for a financial transaction as claimed in any one of claims 11 to 17, including creating a record of the financial transaction for submitting to the financial service provider only after the other of the parties has verified the conducting of the identity checks

19. A method for preparing parties for a financial transaction as claimed in any one of claims 11 to 18, including at the end of some transactions loading a banking card with sums of money that the one of the parties can then use to withdraw at an automatic teller or other money dispensing machine.

20. A financial transaction system for preparing parties for a financial transaction substantially as described herein with reference to the accompanying drawings as appropriate.

21. A method for preparing parties for a financial transaction substantially as described herein with reference to the accompanying drawings as appropriate.