SYSTEM AND METHOD FOR MANAGING REFERRAL WORKFLOWS IN A FINANCIAL INSTITUTION

FIELD OF THE INVENTION

[0001] The present disclosure relates in general to the field of information communication and management, and more particularly, to systems and methods for managing workflows associated with referrals, between a transaction originator and an authorizer.

BACKGROUND OF THE INVENTION

[0002] Financial institutions, unlike any other service industry, require utmost trust and confidence as it deals with customer's money. As a result, financial institutions need to have internal controls and checks with respect to both financial and non-financial transactions. During any such transaction processing, an event may occur which encounters pre-defined instances in the system. An event is used to denote an occurrence of one or more pre-defined business rules. For several transactions in a financial institution, a user handling the request of a customer cannot process a transaction, due to non-overridable events encountered by the system. In such a situation, the financial institution's rules may require the assistance of a second person who will be the authorizer to address the exception raised by the system. Exceptions to these events need to be handled by the financial institution at the earliest as customers may need their transactions to be processed the same day to manage their finances.

[0003] At present, there exists a workflow kind of functionality by which activities can be queued to users. However, intermediate exception authorization cannot be queued using the

workflow as that may lead to a delayed response. Further, exchanging telephone calls, paper based exchanges or sending adhoc mails has a disadvantage of not being able to archive the exceptions and their respective status, for example. Such an approach is highly vulnerable to errors. Further, this may also lead to a delay in response due to improper identification of an authorizer or a delayed response by the identified authorizer.

[0004] With the increasing importance being given to compliance and internal controls, there is a need to have an automated referral infrastructure which provides a mechanism to handle the approval, authorization and escalation process for financial and non-financial transactions in a financial institution, for exceptional events. This would eliminate delays and errors that may happen with manual referrals and escalations, along with transfer of related documents. Further it also helps prioritize work and increase flexibility in the business processes

[0005] Disclosed herein are systems and methods for a referral infrastructure which provides a mechanism to handle the escalation, authorization and approval process for financial and non-financial transactions.

SUMMARY OF THE INVENTION

[0006] Aspects of the disclosure relate to a system and method for managing referral workflows within a financial institution.

[0007] It is therefore one object of the present disclosure to provide systems and methods for automatically controlling and handling the exceptions encountered in a financial institution.

[0008] It is another object of the present disclosure to provide a predefined authorization matrix, to set up controls based on user roles

[0009] It is yet another object of the present disclosure to provide systems and methods which trigger escalation mechanisms.

[0010] The above as well as additional aspects and advantages of the disclosure will become apparent in the following detailed written description

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The aspects of the disclosure will be better understood with the accompanying drawings.

[0012] **FIGURE 1** is a block diagram of a computing device to which the present disclosure may be applied.

[0013] **FIGURE 2** shows an exemplary architecture of a referral management infrastructure.

[0014] **FIGURE 3** shows an exemplary authorization matrix accordingly to the present disclosure.

[0015] **FIGURE 4** shows an exemplary process with the flow of steps for managing referrals.

[0016] **FIGURE 5** shows an exemplary process with the flow of steps for managing escalations, in particular.

[0017] While systems and methods are described herein by way of example and embodiments, those skilled in the art recognize that systems and methods disclosed herein are not limited to the embodiments or drawings described. It should be understood that the drawings and description are not intended to be limiting to the particular form disclosed. Rather, the intention is to cover all modifications, equivalents and alternatives falling within the spirit and scope of the appended claims. Any headings used herein are for organizational purposes only and are not meant to limit the scope of the description or the claims. As used herein, the word "may" is used in a permissive sense (i.e., meaning having the potential to) rather than the mandatory sense (i.e., meaning must). Similarly, the words "include", "including", and "includes" mean including, but not limited to.

DETAILED DESCRIPTION

[0018] Disclosed embodiments provide computer-implemented methods, systems, and computer-readable media for managing referrals in a financial institution. The embodiments described herein are related to financial referrals, and therefore certain pairs of terms ("transaction originator" or "originator" or "user") are used somewhat interchangeably. However, such usage is not intended to limit the present invention to the financial institution. While the particular embodiments described herein to illustrate the invention support financial referrals, the broad principles behind these embodiments could be applied within referral management systems in other fields of endeavor. To facilitate a clear understanding of the present disclosure, illustrative examples are provided herein which describe certain aspects of the disclosure.

However, it is to be appreciated that these illustrations are not meant to limit the scope of the disclosure, and are provided herein to illustrate certain concepts associated with the disclosure.

[0019] It is also to be understood that the present disclosure may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Preferably, the present invention is implemented in software as a program tangibly embodied on a program storage device. The program may be uploaded to, and executed by, a machine comprising any suitable architecture.

[0020] **FIG. 1** is a block diagram of a computing device **100** to which the present disclosure may be applied according to an embodiment of the present disclosure. The system includes at least one processor **102**, designed to process instructions, for example computer readable instructions (i.e., code) stored on a storage device **112**. By processing instructions, processing device **102** may perform the steps and functions disclosed herein. Storage device **112** may be any type of storage device (e.g., an optical storage device, a magnetic storage device, a solid state storage device, etc.), for example a non-transitory storage device. Alternatively, instructions may be stored in one or more remote storage devices, for example storage devices accessed over a network or the internet. The computing device also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the program (or combination thereof) which is executed via the operating system. Computing device **100** additionally may have memory **104**, an input controller **108**, and an output controller **110**. A bus (not shown) may operatively couple components of computing device **100**, including processor **102**, memory **104**, storage device **112**,

input controller **108**, output controller **110**, and any other devices (e.g., network controllers, sound controllers, etc.). Output controller **110** may be operatively coupled (e.g., via a wired or wireless connection) to a display device (e.g., a monitor, television, mobile device screen, touch-display, etc.) in such a fashion that output controller **110** can transform the display on display device (e.g., in response to modules executed). Input controller **108** may be operatively coupled (e.g., via a wired or wireless connection) to input device (e.g., mouse, keyboard, touch-pad, scroll-ball, touch-display, etc.) in such a fashion that input can be received from a user. Of course, **FIG. 1** illustrates computing device **100** with all components as separate devices for ease of identification only. Each of the components may be separate devices (e.g., a personal computer connected by wires to a monitor and mouse), may be integrated in a single device (e.g., a mobile device with a touch-display, such as a smartphone or a tablet), or any combination of devices (e.g., a computing device operatively coupled to a touch-screen display device, a plurality of computing devices attached to a single display device and input device, etc.). Computing device **100** may be one or more servers, for example a farm of networked servers, a clustered server environment, or a cloud network of computing devices.

[0021] When a transaction is being processed by a financial institution the system may raise an event which has resolved in order to proceed with the completion of the transaction. The occurrence of these events is notified in the form of alert messages, to a user who is processing the transaction on behalf of the financial institution. System can be customized to have the facility to define custom alerts based on any parameter, for example, product properties, customer segment, account properties, transaction properties (such as amount, currency, date etc.), the user properties etc. According to one embodiment of the disclosure, alert messages can

be of three types, namely, error messages, warning messages and exception messages. Error messages are those alerts which signify that the data entry is incomplete or incorrect as per the front end validation rules and the associated business rules. A transaction cannot be completed unless the encountered errors are rectified. Warnings are overridable alerts which will pop up as warnings along with their descriptions. The data entry is corrected in these cases as per the front end validation rules and the associated business rules. However, a user can accept the warning, override the alert and proceed to submit the transaction on behalf of a customer. Exception alert messages are those which are not overridable by the user. Exception conditions are classified based on whether the exception condition is related to limits/balances/critical business conditions/environment conditions (like back dated transaction /value dated transaction)/scheme parameters/user parameters etc. These exception conditions are pre-defined by the financial institution. The generation of an exception condition will be used by the system to initiate a referral by forwarding it to the valid authorizers. As used herein, the term 'referral' means generating information regarding the transaction with other necessary information between a transaction originator and one or more transaction authorizers. For security purposes, administrators can restrict what exception instances an authorizer receives. Exception instances are associated with certain types. For example, a bank can setup limits and approval mechanism for the user processing the transaction on behalf of the financial institution when he grants a temporary overdraft to a customer. The approval setup can be done based on different amount slabs thereby helping the bank to setup multiple approvers for high value transactions. Whenever the temporary overdraft is granted, then the overdraft amount is checked with the predefined limit setup for that particular user role and the currency. If the amount is more than the limit, then exception is raised and the user is forced to get approvals. The entire approval process is

automated limiting the user interference. Administrators can assign a user role to an exception type, designated as an authorizer. Optionally, the user can also manually specify the authorizer user id corresponding to different groups of exceptions. A transaction can be referred only when there is a non-overridable exception. If there are no exceptions or if all the exceptions are overridable by the user, it can't be referred. Exception codes are generated based on predefined business events.

[0022] Referring now to **FIG. 2**, which is an exemplary architecture of referral management infrastructure **200** for facilitating management of referrals from a transaction originator to one or more transaction authorizers. A transaction originator may be required to undergo authentication to establish a communication session with the financial institution server before s/he is allowed to access services provided by the server software. The authentication facility directs the server to determine whether the user identified corresponds to an authorized user of the system before establishing a communication session with that transaction originator. A referral process involves a workflow which includes identifying the person authorized to handle any exceptions, tracking and maintaining relevant information pertaining to the generated exception, communicating this information and managing the responses. As used herein, the term transaction originator is a user who is initially handling the transaction request for a customer. An alert action message **202** is generated by the referral message generator module, for an action to be taken by one or more designated transaction authorizers. The alert action message **202** contains most of the information pertaining to a referral and the exception. It should be understood that the alert action message may further include additional information which is nonetheless linked so as to be part of the collection of linked information representing the referral. In a preferred

embodiment, each alert action message contains: (a) Referral ID - unique identifier for each referral; (b) Referral Description-Contains the details relating to Entity & the description of the non overridable exception; (c) Originator Id-User id of the transaction originator; (d) Date & Time of the referral. The alert action message **202** will be processed by referral router module **204**, which will receive the alert action message and further route the alert action message to the designated authorizers. The referral router identifies the particular sequence or the required sequence of the associated authority matrix **206**. As used herein the term authorizer denotes one or more authorizers to whom the alert action message is routed, via a referral router **204**. Seeking assistance of an authorizer involves the system identifying a suitable authorizer as per a pre-defined, associated authority matrix **206**. Alternatively, the system may be configured to manually create referrals by selecting an option such as a referral button. The referral button will cause the terminal and server to cooperate to create an alert action message. Referral inbox module **208** displays all the active referrals corresponding to the transaction originator or the authorizer. The method includes the steps of routing an alert action message **202** to at least one authorizer and subsequently automatically updating the referral inbox **208** with the alert action message and its status regarding the actions taken by one more authorizers. An authorization step requires designated individuals to take action on the exception. The referral infrastructure is enabled only for those exceptions that are linked to a particular authorization matrix **206**. The referral infrastructure, in addition, has a mechanism to escalate the referrals that are lying with an authorizer or a role to another role after a specified period of time. The referral management system needs an action to be taken by the authorizer keeping the referral message. Where no action has been taken, an escalation is registered under an escalation program **210** in the referral management system. As used herein, the term Escalation denotes a means of notifying a new set

of authorizers of an escalation action message, generated by the message generator module. The message generator module, in principal, generates alert action messages and escalation action message. The nature of the two types of action messages is somewhat similar, with the escalation action message bearing additional information regarding the escalation details.

[0023] A transaction originator may alternately act as a customer imitating the transaction on their own or an authorizer, in different transactions. Accordingly, a terminal in this system is typically operable to both send and receive referral messages, which include, alert action message and escalation action messages. Thus, the characterizations used herein of a terminal being either a transaction originator or authorizer should be understood as being descriptive only in respect of particular transactions performed from the terminal involving either the sending or receiving of a referral message, respectively. In other words, the same terminal could be characterized as a referrer computer in one transaction but as a referee computer in another.

[0024] FIG. 3 shows an exemplary authorization matrix accordingly to the present disclosure. There are a number of inputs to the authorization process, which includes delegation, inferred by the referral router **204.** Within the business rules, the designated individuals may be identified in what is referred to as an authorization matrix **300**. As used herein, the term authorization matrix is a matrix of individuals and business events. It includes a set of group expressed through each row, along with a set of exceptions. This could include, for example, a hierarchy of a financial institution. Whenever the financial institute validates any transaction and raises an exception code for which a matrix is linked, then it will follow the authorization matrix **300**. Mapping of a business event with the authorization matrix may not be needed in this case, i.e. authorization

matrix will be directly mapped to exception codes and will not require any mapping with the underlying exception events conditions, predefined by the financial institution. In the exemplary embodiment, each individual or group of individuals of system is assigned to one or more roles. As used herein, the term role describes a permission to perform any one of a defined set of business events. Each role includes a set of designated privileges. An authority matrix **300** is created and managed by an administrator whose operation causes the terminal and server to cooperate to permit a user, transaction originator or an authorizer, to take action for an exception. The exception is validated against a list of rules, and if valid, is sent for storage to the referral inbox **208**, a copy of which goes to the transaction originator and an authorizer. A financial institution will be able to assign an authority matrix to the exception codes (to form an associated authority matrix). The associated authority matrix includes at least one authorizer and an exception code to be handled by the designated authorizers. If an individual designated by the authority matrix leaves for a vacation, that individual may delegate approval to an available individual. An authorization matrix will have referral routing information like, authorization levels & escalation steps and user roles that can authorize an exception or a deviation at an authorization level. Authorizations are carried out only in a serial manner i.e. only after authorization is done at first level (level 1), referral will be sent to the next level (R_{n+1}). Preferably, one individual should not be allowed to authorize the same exception at two different authorization levels. For instance, consider that the role R2 (Manager) is defined as authorizer at escalation step 1 of authorizer level 1 as well as at the authorization level 2 in the associated authorization matrix **300**. In this case if a manager (of role R2) authorizes the exception at escalation step 1 of level 1, then the same manager, when he receives message to authorize the same exception at authorization level 2 (since R2 is also defined as authorizer at level 2), s/he

should not be allowed to authorize that exception. It is to be understood by one of ordinary skill in the art that the role (R2) can take multiple roles in each step.

[0025] FIG. 4 shows an exemplary process with the flow of steps for managing referrals. Consider, for example, a transaction originator) initiating a transaction **402** with a bank for issuing a demand draft. In the backend, the bank may have setup limits and approval mechanism (based on the business events) for a particular transaction originator when s/he changes the system level charges & commission setup for a customer. The approval setup has been done based on different amount slabs thereby helping the bank to setup multiple approvers for high value transactions. Whenever the charge amount is modified, then the charge amount is checked with the predefined limit setup for that particular transaction originator's role and the currency. When the transaction originator submits the transaction to the system **404,** the system may throw three types of alerts **406.** If the alert type is an error, then the transaction originator examines the error **408** and rectifies the error by modifying the transaction **410.** A transaction cannot be completed unless the encountered errors are rectified. Once rectified, the transaction originator can resubmit the transaction to the system **404.** If the alert type is a warning, then the warning will pop up as warnings along with their descriptions. The transaction originator must accept the warning **412,** override the alert and proceed to submit the transaction **414** on behalf of a customer. If the alert encountered is an exception type, then the system can be configured to check whether the transaction originator can review the exception on his own **416.** If the administrator has permitted the transaction originator's role to handle such an exception code, then the transaction originator has the responsibility of reviewing the transaction and take appropriate actions **418.** The transaction originator reviews the alert action message to either

approve the referral and submit the transaction to the system **414** or decline and accordingly modify the transaction **420** and submit the transaction to the system **404.** The approval action is a status indicating that the exception represented has been approved for by the transaction originator. If the transaction originator is not authorized to review situation, then a referral message (alert action message) is generated **422** by the referral message generator module **202.** The alert action message is routed through the authorization process according to a referral router **204** that identifies the person-to-person sequence. The referral inbox **208** will display a list of incoming and outgoing referral messages (alert action message/escalation action message) for which the action has to be taken or has been acted upon. The transaction originator can always view the referral message from his referral inbox rather than saving a copy on the local system or making an effort to save a copy in the central location. The actions taken by the authorizers will also be visible to the transaction originator in this way. According to one embodiment of the disclosure, the referral inbox is divided into two sections namely, referred to me and referred by me. Referred to me shows the list of referrals which are referred to the designated authorizers and for his action. Referred by me section shows the list of referral which are initiated by the transaction originator. The referral inbox **208** is operable to store the referral status information, and to set the referral responses to a value indicating that the referral message has not yet been viewed by the transaction originator or the authorizer, as the case maybe. A referral response is based on the actions taken by the one or more authorizers as per the associated authority matrix **300**. The actions represent the status associated with the referral messages (alert action message/escalation action message). These response types drive the referral messages from one state to another in the authority matrix **300**. The system automatically sends the referral message (alert action message/escalation action message) to the first authorizer as per the associated

authority matrix **300.** Once the referral message reaches the authorizer, the designated authorizer has to take an action **424.** The authorizer can take the following actions for the transaction: (a) Hold: a status indicating that the exception represented by the referral is on hold, for further verification **426a**. When a referral is on hold then it is not allowed to escalate to other levels after a fixed duration of time. No other authorizer will be able to view the referral as it is on hold. In one exemplary embodiment of the disclosure, the administrator can release the referral kept on hold. If the authorizer wants to release the hold **426b**, then s/he must take an action **424** accept, decline or forward the referral. By selecting forward as an option (not shown), the designated authorizer reroutes the referral to a particular authorizer. The forwarded to authorizer will now be able to view the referral in his inbox and can take action on it; (b) Decline: a status indicating that the exception represented by referral message has been declined and the transaction has been cancelled. No other authorizer will be able to view the referral in his or her inbox. The transaction originator can now withdraw the referral or withdraw and modify the transaction **428.** By deciding to withdraw the referral, the transaction originator is essentially deleting the referral **430** and the transaction will no longer be available. Alternatively, the transaction originator can withdraw and modify the transaction deleting the referral **432** and modifying the transaction **410**; (c) Approve: a status indicating that the exception, represented by the referral message has been approved by the designated authorizer. After the authorization the users belonging to the role in the next level will be able to view the referral in their inbox. If the associated authority matrix does not have a valid authorizer (i.e. R_{n+1}) **434**, then the referral message, along with the respective responses of the designated authorizers is sent to the transaction authorizer. The transaction authorizer can view these responses from the referral inbox. The transaction originator can now take three types of actions **436.** The originator can submit the transaction

when the referral has been approved. When all the authorization in the referral is completed the transaction originator will see the status as approved. The transaction originator can now submit the transaction from referral inbox. This would complete the transaction cycle. Alternately, the transaction originator can now withdraw the referral or withdraw and modify the transaction. By deciding to withdraw the referral, the transaction originator is essentially deleting the referral **430** and the transaction will no longer be available. Alternatively, the transaction originator can withdraw and modify the transaction deleting the referral **432** and modifying the transaction **410**

[0026] FIG. 5 illustrates an escalation mode of a referral management system in accordance with an embodiment of the present disclosure. Considering the same example taken for the referral workflow, a transaction originator (or a customer) initiating a transaction **502** with a bank for issuing a demand draft. When the transaction originator submits the transaction to the system **504,** the system may throw three types of alerts **506.** If the alert type is an error, then the transaction originator examines the error **508** and rectifies the error by modifying the transaction **510.** Once rectified, the transaction originator can resubmit the transaction to the system **504.** If the alert type is a warning, then the transaction originator must accept the warning **512,** override the alert and proceed to complete the transaction **514** on behalf of a customer. If the alert encountered is an exception type, then the system can be configured to check whether the transaction originator can review the exception on this own **516.** If the administrator has permitted the transaction originator's role to handle such an exception code, then the transaction originator has the responsibility of reviewing the transaction and take appropriate actions **518.** The transaction originator reviews the alert action message to either approve the referral and submit the transaction to the system or decline and accordingly modify the transaction and

submit the transaction to the system. The approval action is a status indicating that the exception represented in the referral has been approved for by the transaction originator. If the transaction originator is not authorized to review situation, then a referral message (alert action message) is generated **520** by the referral message generator module **202.** The alert action message is routed through the authorization process according to a referral router **204** that identifies the person-to-person sequence **522**. Alternatively, originator can then forward the referral to a specific authorizer. If the designated authorizer takes action within a predetermined time period **524,** designated authorizer belonging to the role in the next level **526** will be able to view the referral in their referral inbox. If the associated authority matrix does not have a valid authorizer (i.e. R_{n+1}), then the referral message, along with the respective responses of the designated authorizers is sent to the transaction authorizer. If the approval has been obtained from all designated authorizers as per the associated authority matrix, the status of the referral, along with the responses of the respective authorizers is reflected in the in the referral inbox of the transaction originator. The transaction originator at this point of time, is mandated to take an action to submit the transaction, withdraw the transaction, withdraw and modify the transaction, as the case maybe. If the designated authorizer does not respond within a predetermined time period **524**, then the escalation program **210** is automatically initiated **528**. Once escalated, the escalation program is initiated and an escalation action message is generated **530**. The escalation action message is sent to the first authorization role corresponding to that authorization level of associated authorization matrix **300**. For example, if a referral is sent for authorization to users of role R1 at authorization level 1 and if no one belonging to role R1 authorizes the referral, then after specified time, the referral gets escalated to escalation step 1 of level 1 which has role R2 as authorizer. During this escalation, referral will be removed from all the R1 users' inbox and will

be displayed in all the R2 users' inbox. The escalation mode is automatically triggered by the system based on pre-determined qualifiers such as time period, for example. The period for a given escalation is monitored by the system using timer tasks, for example. The length of pre-determined time duration Referrals that are on hold will not be escalated. Based on the level, escalation step in which the referral is lying; it will be escalated to the role in the next escalation step **526**. If there is no next role available, then the referral is returned back to the transaction originator **518**. The transaction originator will see this referral in the referred to me section in the referral inbox. The transaction originator can now forward this to a specific user available for approval in that particular level. If the next role is available as per the associated authority matrix, then the designated authorizer would have to take action on the referral **532.** This would continue again from **522** till all approvals required are obtained.

[0027] These embodiments may be implemented with software, for example modules executed on computing devices such as computing device **300** of **FIG. 3**. Of course, modules described herein illustrate various functionalities and do not limit the structure of any embodiments. Rather the functionality of various modules may be divided differently and performed by more or fewer modules according to various design considerations.

[0028] Having described and illustrated the principles of the disclosure with reference to described embodiments and accompanying drawings, it will be recognized by a person skilled in the art that the described embodiments may be modified in arrangement without departing from the principles described herein.

CLAIMS

What is claimed is:

1. A computer-implemented method for managing referral workflows in a financial institution, the method comprising:

receiving an inbound communication of a user, wherein the inbound communication comprises data pertaining to the user's transaction with the financial institution;

generating a referral alert action message on the event the processing of the inbound communication leads to a non-overriding alert, wherein the referral alert message is generated by a transaction originator;

automatically routing the referral alert message to a first alert authorizer identified from one or more authorizers of an associated authority matrix, wherein the one or more authorizers are financial assistance providers of the financial institution;

automatically routing the referral alert message to a subsequent alert authorizer identified from the one or more authorizers of the associated authority matrix on the event a response has been received from the first alert authorizer; and

routing the response from each of the one or more authorizers to the transaction originator for taking an action pertaining to the inbound communication,

wherein the associated authority matrix comprises the one or more authorizers and associates the one or more authorizers with one or more exception codes to be handled by the one or more authorizers.

2. The computer-implemented method of claim 1, wherein the referral alert message is routed to a referral inbox of the one or more authorizers and the transaction originator.

3. The computer-implemented method of claim 1, wherein the non-overriding alert is a predefined business event.

4. The computer-implemented method of claim 1, wherein a referral escalation message is generated in the event the one or more authorizers fail to take action on the referral alert message in a predetermined time period.

5. The computer-implemented method of claim 4, wherein the referral escalation message is routed to a first escalation authorizer identified from the one or more authorizers of the associated authority matrix.

6. A system for managing referral workflows in a financial institution, the system comprising:

an input terminal for receiving an inbound communication of a user, wherein the inbound communication comprises data pertaining to the user's transaction with the financial institution;

a computing system communicating with the input terminal comprising:

a referral message generator module for generating a referral alert message on the event the processing of the inbound communication leads to a non-overriding alert, wherein the referral alert message is generated by a transaction originator;

an associated authority matrix module, wherein the associated authority matrix comprises one or more authorizers eligible to receive the referral alert message; and

a message router module to automatically route the referral alert message to the actors who are associated with authority matrix mapped to the non-overriding alert; and

a referral inbox module to display information on the status of the referral alert message,

wherein the non-overriding alert comprises at least one exception code,

wherein the one or more authorizers are associated with one or more exception codes, and eligibility of the one or more authorizers is determined based on the associated authority matrix and the non-overriding alert's at least one exception code.

7. The system of claim 6, wherein the referral alert message is automatically routed to a first alert authorizer identified from the associated authority matrix.

8. The system of claim 7, wherein the referral alert message is routed to a subsequent alert authorizer of the associated authority matrix on the event a response has been received from the first authorizer.

9. The system of claim 8, wherein the referral message module is further adapted to generate a referral escalation message in the event the one or more authorizers fail to take action on the referral escalation message in a predetermined time period.

10. The system of claim 9, wherein the referral escalation message is routed to a first escalation authorizer identified in a predefined order from the one or more authorizers of the associated authority matrix.

11. The system of claim 6, wherein the referral alert message is routed to the referral inbox of the one or more authorizers and the transaction originator.

12. The system of claim 6, wherein the non-overriding alert is a predefined business event.

13. A computer readable medium having a set of instructions for execution on a computing device, the set of instructions comprising:

a referral message routine for generating a referral alert message on the event the processing of an inbound communication of a user leads to a non-overriding alert, wherein the referral alert message is generated by a transaction originator, wherein the inbound communication comprises data pertaining to the user's transaction with the financial institution;

an associated authority matrix routine, wherein the associated authority matrix comprises one or more authorizers eligible to receive the referral alert message;

a message router routine to automatically route the referral alert message to the associated authority matrix; and

a referral inbox module to display information on the status of the referral alert message,

wherein the non-overriding alert comprises at least one exception code,

wherein the one or more authorizers are associated with one or more exception codes.