AA EXCHANGE®

Fraud Prevention Policy

Version: 2.4 (2024)

Dated: February 08, 2024

TABLE OF CONTENTS

INTRODUCTION (PURPOSE & SCOPE)

Instances of corporate fraud and misconduct remain a constant threat to the company for public trust and confidence. In order to maintain goodwill, public trust and to strengthen the company's high standards, controls have been introduced and implemented to provide an environment which will minimize the risks for fraud. These procedures and controls help AA Exchange Company (Pvt) Ltd. (the company) to maintain goodwill, high standard, public trust and confidence.

While acknowledging that no single approach to fraud risk management can fit for the organization's needs, this document spotlights key practices that company has generally found to be effective, when tailoring the specific antifraud program, and offers a strategic approach to aligning corporate values with performance.

AA Exchange Company's antifraud policy and guidelines is focusing on following factors.

- Understand the fraud and misconduct risks that are associated with the company offered services including:
    - International Money Transfer (Send/Receive)
    - Foreign Telegraphic Transfer and Foreign Demand Draft
    - Foreign Currency Exchange
    - Branchless Banking
- Determine whether antifraud programs and controls are effective in reducing instances of fraud and misconduct
- Gain insight on better ways to design and evaluate controls to prevent, detect, and respond appropriately to fraud and misconduct
- Reduce exposure to sanctions, corporate liability, and litigation that may arise from violations of law or regulator expectations
- Derive practical value from compliance by creating a sustainable process for managing risk and improving performance
- Achieve the highest levels of business integrity through internal control, transparency and sound corporate governance.

KEY OBJECTIVES

The Company, fraud risk management approach encompasses controls that have three objectives:

- **Prevent**. Reduce the risk of fraud and misconduct from occurring.
- **Detect**. Discover fraud and misconduct when it occurs.
- **Respond**. Take corrective action and remedy the harm caused by fraud or misconduct.

PULLING IT ALL TOGETHER

The challenge for the company is to develop a comprehensive effort to:

- Understand all the various control frameworks and criteria that apply to the company.
- Classify risk assessments, codes of conduct, and develop mechanisms for the company objectives.
- Create a wide-ranging program that manages and integrates fraud prevention, detection, and response efforts.

AN ONGOING PROCESS

Effective fraud risk management provides the company with tools to manage risk in a manner consistent with regulatory requirements as well as the entity's business needs and regulators expectations. Such an approach has four phases:

Assess Risks. Identifying the scope of the analysis and key stakeholders, profile the current state of fraud risk management, set targets for improvement, and define steps necessary to close the "gap."

Design. Developing a wide-ranging program that encompasses controls to prevent, detect, and respond to incidents of fraud or misconduct.

Implement. Deploying a strategy and process for implementing the new controls throughout the company and assign responsibility for leading the overall effort to a senior individual.

Evaluate. Assessing existing controls compared with legal and regulatory frameworks as well as leading practices, such as internal investigation protocols or due diligence practices.

DEFINING FRAUD AND MISCONDUCT

Fraud is an intentional act by one or more individuals/entities, involving the use of deception to take an unjust or illegal advantage. Merely, fraud is an act of deception intended for personal gain or to cause a loss to another party. It is a type of criminal and illegal activity, defined as:

'Abuse of position, or false representation, or prejudicing someone's rights for personal gain'.

Fraud is a broad legal concept that generally refers to an intentional act committed to secure an unfair or unlawful gain.

Misconduct is also a broad concept, generally referring to violations of laws, regulations, internal policies, and market expectations of ethical business conduct.

Together, they fall into the following categories of risk that can undermine public trust and damage a company's reputation for integrity:

- Misappropriation (e.g., embezzlement, external theft, counterfeiting)
- Fraudulent reporting
- Revenue or assets gained by fraudulent or illegal acts (e.g., over-billing customers, deceptive sale purchase of foreign currency)
- Expenses or bills recorded overstated or understated
- Expenses or liabilities incurred for fraudulent or illegal acts (e.g., commercial or public bribery)
- Other misconduct (e.g., conflicts of interest, insider trading, discrimination, theft of competitor's trade secrets, antitrust practices)

Furthermore, internally, employees can abuse the trust and take advantage/commit fraud against the company, seeing an exploitation opportunity or an employment opportunity it can include activities that are in violation of or non-compliant with Local and International laws, regulations, policies and procedures and externally fraudsters/impostors are always finding different means to trick you out of your money. They could target through emails, phone calls, letters, and social networking sites.

ROLES AND RESPONSIBILITIES

The company has designed roles and responsibilities with respect to frauds of various stakeholders like staff, vendors dealing directly and indirectly with the company including Board of Directors.

BOARD OF DIRECTORS

Company board of directors plays an important role in the oversight and implementation of controls to mitigate the risk of fraud and misconduct. The board, together with management, is responsible for setting the "tone at the top" and ensuring support is established at the highest levels for ethical and responsible business practices.

Directors have not only a fiduciary duty to ensure that company has programs and controls in place to address the risk of wrongdoing, but also a duty to ensure that such controls are effective.

SENIOR MANAGEMENT

To help ensure that fraud and misconduct controls remain effective and in line with regulatory standards, responsibility for the company fraud and misconduct risk management approach should be shared at senior levels (i.e., individuals with substantial control or a substantial role in policy-making). This critical oversight begins with prevention and must also be part of detection and response efforts.

The chief executive officer shall ensure that the compliance department is adequately resourced and trained to detect and mitigate the risks of fraud in the company.

COMPLIANCE DEPARTMENT

Responsibility for antifraud efforts will reside with the compliance team who works together with internal audit staff and designated subject matter experts. Compliance department is responsible for coordinating the Company approach to fraud and misconduct prevention, detection, and response. When fraud and misconduct issues arise, the department will draw together the right resources to deal with the problem and make necessary operational changes. The designated Compliance manager may also chair a meet of cross functional managers who:

- Coordinate the Company risk assessment efforts
- Establish / amend policies and standards of acceptable business practice
- Oversee the design and implementation of antifraud programs and controls
- Report to the board and/or the audit committee on the findings of the company fraud risk management activities to take appropriate measure.

Other manager's such as departmental heads (e.g., Human Resource, Marketing, Accounting, and Administration) can also participate in responsibilities under the company antifraud strategy, they oversee areas of daily operations in which risks arise. Such department heads can serve as subject matter experts to assist the compliance manager with respect to their particular areas of expertise or responsibility.

INTERNAL AUDIT FUNCTION

In AA Exchange Company, internal audit function is a key participant in antifraud activities, supporting management's approach to preventing, detecting, and responding to fraud and misconduct. Such responsibilities represent a change from the more traditional role of internal audit (that is, examining the effectiveness of the company internal controls). In general, internal audit should be responsible for:

- Conducting the evaluation of design and operating effectiveness of antifraud controls
- Assisting in the company fraud risk assessment and helping draw conclusions as to appropriate mitigation strategies
- Reporting to the audit committee on internal control assessments regarding fraud, audits, investigations, and related activities.

FRONT LINE ASSOCIATES (FLA) AWARENESS & RESPONSIBILITIES

Mitigating the fraud began with the person who is dealing directly with customers. i.e. Front line associates (FLA). Therefore, front line associates FLAs shall be adequately trained to help identify the types of fraud, transactions, and consumer behavior that specify a consumer may be a victim of fraud as they are the first, last, and best line of defense against scammers. If the consumer's responses, behavior or transaction patterns indicate that they may be a victim of fraud, then FLA can refuse to send the transaction.

CONSUMER PROTECTION & AWARENESS

FLA shall endeavor to educate customers on safeguarding transactions and personal information, and evading fraud when using our services.

If customers are processing transactions for/to someone they don't know personally, they could be possibly a victim of fraud. Ensure and remind customers to secure themselves and their money.

CONSUMER FACING MATERIALS

Awareness posters and leaflets should be clearly displayed at the location.

BROCHURE

The brochure provides tips and scenarios to help FLA at POS in preventing fraud.

Fraudsters are using the internet, the mail, and the telephone to have victims fall victim to their scams. It's important to remember that fraudsters are ingenious at gaining their victims trust and gathering personal information.

USER MANAGEMENT SECURITY

- Passwords should be changed on regular basis
- User IDs and passwords should never be shared
- Employees MUST manually log off the system when it is not in use

- Protect user information. Do not divulge confidential information to anyone based on an incoming telephone call

TRANSACTIONS SECURITY

- Do not discuss any aspect of the international money transfer services, foreign currency or Foreign Telegraphic Transfer / Foreign Demand transactions, including specific money transfer details, with anyone other than the Sender, or authorized representatives.
- Only the authorized representatives at Head Office will ask FLA for the Account Number, Terminal ID, Operator ID, or password.
- Never provide information regarding money transfers to anyone on a telephonic request
- FLA must contact relevant department at Head Office if receive a phone call requesting remote access of the system, Head of that department shall verify the authenticity of the caller
- True customer must be present. Also, do not execute transactions over the telephone.
- Before executing any transaction, verify that the proper amount of valid currency to cover principal and charges is received.
- FLA must contact the relevant department at Head Office for any modifications in the money transfer. The department shall then require necessary documents (modification form (if any) and other supporting documents) to process any corrections in a money transfer
- No one other than the technical support team at Head office will call the FLA to enter codes into the system to fix a technical issue.

CASH RECEIVED/PAID

FLA on the counter is responsible for Cash Received/Paid to process any transaction.

RECONCILIATION

Must reconcile daily to identify fraud or internal theft and immediately report any discrepancies to Head Office.

REDUCING THE RISK OF FRAUDULENT ACTIVITIES

Before processing any transaction, you must always ensure that the customer provides complete and all the required information. Please follow the payout and send money procedure.

ACCEPTABLE FORMS OF IDS

- For Pakistan National: CNIC / SNIC /NICOP / POC / Passport
- For Foreign National: Passport + Valid Visa
- For Afghan National: POR / ARC / Passport + Valid Visa

If the Agent/FLA fails to verify the transaction information, there is a risk that the transaction may be paid in error (to the wrong payee). For further details, please review the Payment Exceptions, including, but not limited to, the Streamlined Payout Policy ("SPP"). FLA must contact CSC at Head office for any questions or queries. However, in case the transaction is paid in error, FLA must contact CSC immediately to reinstate the same on urgent basis to avoid any Fraudulent Activity/Non-Payment Claims.

TRANSACTION FRAUD INDICATORS – PAY SIDE

The FLA should be aware of the following examples of types of transactions, and ask the consumer additional questions about the transaction, because they may be evidence of a fraud or other crimes.

- Consumers who receive transactions under different names or spelling variations.
- Consumers who receive non-standard or unusual transaction amounts in a short period of time.
- Consumers who receive an unusually high number of transactions in a short period of time.
- Consumers who receive multiple transactions requiring a security question.
- Consumers who receive multiple transactions from multiple senders with no apparent family relationship.

TRAINING AND MONITORING

TRAINING

Company has applied adequate training programs to ensure that its Branch staff understand the obligations, particularly about detection and prevention of fraud. Compliance department shall ensure that staff must be fully trained and educated on types of fraud its detection and prevention before conducting any transaction; the training programs shall include at least the following areas:

- Understanding the objective to the company anti-fraud program
- Recognize the different types of consumer fraud and how it works
- Steps to Identify Frauds & Prevention of Fraud
- Steps you should take when you suspect consumer fraud – sender side
- Steps you should take when you suspect consumer fraud – receiver side
- Understand your obligations as a staff of AA Exchange Company
- Understand how you can prevent your customers who may be victims of fraud

Branches staff training should be documented, and training records should be maintained according to Company's record keeping requirements. Compliance Manager may interview FLAs in order to determine that whether staff are adequately trained.

Trainings shall be provided in the following manner:

- At the time of induction, staff will be provided with the basic training including anti-fraud program.
- FLA are required to be trained on anti-fraud program before executing any financial transaction.
- Trainer should include easy and understandable material considering the local and international guidelines for fraud prevention.
- At every quarterly internal audit, the onsite auditors will provide on the job refresher training (OJT) covering anti-fraud policy and operations.

- Compliance team may conduct offsite / online training preferably on bi-annual basis (Or as and when deemed necessary).
- On job training (OJT) of staff.
- Annual trainings may be conducted by the company, where departmental heads and specialists from different fields shall provide training including company's anti-fraud prevention program.
- In addition, various training sessions will be conducted throughout the year at different level.

MONITORING

Branches shall be reviewed periodically during the compliance review or by onsite internal audit inspection. Staff will be penalized, suspended or terminated that are not operating in line with the company's fraud prevention policy. Related measures include the following:

a) Extensive internal audit and risk assessment
b) Mystery Shopping
c) Extensive transactions monitoring
d) Especially designed fraud posters/customer information display cards etc. inside locations' enabling FLAs and customers to understand regulatory and Foreign Associates requirements
e) Fraud Awareness Posters
f) Dedicated teams and telephone lines to handle fraud and customer complains

AA Exchange has adequate monitoring system in place for all its branches and subagents. Relevant team at head office maintain "Fraud Log" which shall be reviewed by compliance manager periodically.

EMPLOYEE AND THIRD-PARTY DUE DILIGENCE

An important part of company fraud and misconduct prevention strategy is the use of due diligence in the hiring, retention, and promotion of employees, agents, vendors, and other third parties. Such due diligence may be especially important for those employees identified as having authority over the financial reporting process.

The scope and depth of the due diligence process typically varies based on the identified risks, the individual's job function and/or level of authority, and the specific laws set by state bank of Pakistan.

There are certain situations where screening third parties may be valid. For example, management may wish to screen agents, consultants, or temporary vendors who may access confidential information or acquisition targets that may have regulatory or integrity risks that can materially affect the value of the transaction.

Due diligence begins at the start of an employment or business relationship and continues throughout. For instance, taking into account behavioral considerations such as adherence to the company core values in performance evaluations provides a powerful signal that management cares about not only what employees achieve, but also that those achievements were made in a manner consistent with the company's values and standards.

Employees symbolize the company's standards and their ethics and behaviors affect the company's reputation. However, employees can commit fraud against the company, seeing an opportunity to obtain benefits.

To protect the company from getting affected from the inside, ensure and verify the complete background of the employee keeping in view the threats they can bring, before employment.

Assigning of Operator ID

- Assign each employee with a unique Operator ID and password
- When one of the employees is terminated, his/her operator ID must be immediately deleted from the system

PREVENTION AND DETECTION OF FRAUDS AGAINST CONSUMER & AGENTS

In order to mitigate the risk of fraud, FLAs must assess every transaction for suspicious activity and report any fraudulent transactions to Head office that seem suspicious.

PREVENTING MONEY TRANSFER FRAUD AGAINST CONSUMERS

Company has implemented active plan to prevent consumer fraud. Consumer fraud occurs when criminals convince or trick consumers to transfer money to the criminal or the criminal's associates. Criminals use a variety of scams to perpetrate such crimes, and they often target the most vulnerable members of society—particularly the elderly. It is therefore imperative that staff are always aware of potential fraud-related activity.

Consumer fraud generally involves criminals conducting scams to persuade consumers to transfer money to them that might sound financially appealing to the consumer but are in fact an attempt to steal from the consumer. Most consumer fraud involves the victim's perception that they will receive some sort of financial gain or that they are helping a friend, relative, or loved one. A common theme in all consumer fraud schemes is that the consumer has never met the receiver in person. All staff must take the steps described in this policy to detect, deter, and report consumer fraud. However, staff should understand the below mentioned types of fraud in order to prevent the customers.

COMMON CONSUMER FRAUD TYPES

All staff must be trained to recognize the following common types of consumer fraud scams, so they can help protect consumers from becoming victims.

Advanced Fee or Prepayment Scam

Victim is asked to pay upfront fees for financial services which are never provided. Victims often send a succession of transactions for payment of various upfront fees. Methods: credit card, grant, loan, inheritance, investment.

Anti-virus scam

Victim is contacted by someone claiming they are from a well-known computer or software company and a virus has been detected on the victim's computer. The victim is advised that the virus can be removed, and the computer protected for a small fee with a payment by either credit card or a money transfer. There was no virus on the computer and the victim has just lost the money they sent for the protection.

Charity scam

The victim is often contacted by e-mail, mail or phone by someone asking for a donation to be sent by money transfer to an individual to help victims of a recent current event, such as a disaster or emergency (such as a flood, cyclone, or earthquake). Legitimate charity organizations will never ask for donations to be sent from one individual to another individual through a money transfer service.

Emergency Scam

Victim is led to believe that they are sending funds to assist a friend or loved one in urgent need. Victim sends the money with urgency as the victim's natural concern for a loved one is exploited.

Employment Scam

Victim responds to a job posting and is hired for the fictitious job and sent a fake cheque for job related expenses. Cheque amount exceeds the victim's expenses and victim sends remaining funds back using a money transfer. The cheque bounces and the victim is responsible for the full amount.

Fake (Counterfeit) Cheque Scam

Victims are often sent a cheque as a part of a scam and told to deposit the cheque and use the funds for employment expenses, internet purchases, mystery shopping, etc. The cheque is fake (counterfeit), and the victim is left responsible for any funds used from the cheque. Remember, funds from a cheque deposited into an account should not be used until the cheque officially clears, which can take weeks.

Grandparent Scam

This scam is a variation on the Emergency Scam. The victim is contacted by an individual pretending to be a grandchild in distress, or a person of authority such as a medical professional, law enforcement officer, or attorney. The fraudster describes an urgent situation or emergency (bail, medical expenses, emergency travel funds) involving the grandchild that needs a money transfer to be sent immediately. No emergency has occurred, and the victim who sent money to help their grandchild has lost their money.

Immigration Scam

Victim receives a call from someone claiming to be an immigration official saying there is a problem with the victim's immigration record. Personal information and sensitive details related to the victim's immigration status may be provided to make the story seem more legitimate. Immediate payment is demanded to fix any issues with the victim's record and deportation or imprisonment may be threatened if payment is not made immediately by money transfer.

Internet Purchase Scam

The victim sends money for the purchase of item ordered online (e.g. pets, cars). Items are often advertised on Craigslist, eBay, Alibaba, etc. After the money is sent, the victim never receives the merchandise.

Tax Scam

Victim is contacted by someone claiming to be from a governmental agency saying that money is owed for taxes, and it must be paid immediately to avoid arrest, deportation or suspension of driver's license/passport. The victim is instructed to send a money transfer or purchase a pre-loaded debit card to pay the taxes. Government agencies will never demand immediate payment or call about taxes without first having mailed a bill.

Lottery or Other Prize Scam

Victim is told that they have won a lottery, prize or sweepstakes and that money must be sent to cover the taxes or fees on the winnings. The victim may receive a cheque for part of the winnings and once the cheque is deposited and money is sent, the cheque bounces.

Mystery Shopping Scam

The fraudster contacts the victim through an employment website, or the victim responds to an ad about an employment opportunity to evaluate a money transfer service. The fraudster often sends the victim a cheque to deposit and instructs the victim to send a money transfer, keeping a portion of the cheque for their pay. The victim sends the money, the fraudster picks it up, and when the cheque bounces the victim is left responsible for the full amount.

Overpayment Scam

The fraudster sends the victim a cheque that appears to be valid as payment for a service or product. Typically, the amount of the cheque exceeds what the victim expects to receive, and the fraudster tells the victim to send the excess back using a money transfer. When the cheque bounces, the victim is left responsible for the full amount.

Relationship Scam

Victim is led to believe that they have a personal relationship with someone they met online often by social media, in an online forum or on a dating website. The victim is often emotionally invested, often referring to the recipient as a fiancée and believes they are sending money for travel or medical expenses. In the end, the fraudster is stealing from the victim and no relationship is every formed

Rental Property Scam

Victim sends money for deposit on a rental property and never receives access to the rental property or the victim may also be the property owner who is sent a cheque from the renter and asked to send a portion of the cheque back using a money transfer and the cheque bounces.

NOTE: All elder and dependent adult consumers should be asked if they have met the person they are sending money to because they are highly vulnerable to telephone or online fraud. If it becomes clear that the sender is not sure if the receiver is legitimate, then the Associate should refuse to process the transaction. If the elder person is sending to a grandchild, the Associate must always ask the grandparent if they have called their grandchild to verify that the emergency is real.

Telemarketing Fraud

Any type of fraud scheme in which a criminal communicates with the potential victim via the telephone. The criminal then uses the credit card information to make unauthorized purchases and the victim never sees a dime.

Examples:

- A telemarketer fraudster may tell you: "You must act 'now' or the offer won't be good."
- "You've won a 'free' gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You can't afford to miss this 'high-profit, no-risk' offer."

REQUIREMENTS WHEN ENCOUNTERING RED FLAGS FOR FRAUD

Careful observance of consumer behavior is an important function in identifying potentially illegal or fraudulent activity. A "red flag" is a noticeable situation or fact that could indicate fraudulent or illegal behavior. Red flags may be noted by observing a consumer's behavior. For example, a consumer may act nervous, apprehensive, or confused, or be reluctant or unable to provide basic details about the sender, receiver, or purpose of the transaction. Other times the consumer may not know specific details related to their transactions. The consumer may conduct multiple transactions in small or odd amounts, or multiple transactions to multiple receivers in various locations.

Below are some examples of consumer fraud red flags. These red flags are provided as guidelines for preventing fraud, if the staff notices any consumer fraud red flags and suspects that the receiver may be picking up a fraudulently induced transaction, staff may perform the following actions:

- Ask additional, KYC questions with the purpose of making the receiver think about their responses. Pay attention to not only the receiver's answers to the questions, but also the receiver's behavior (do they become nervous or struggle to answer?). Examples of KYC questions are:
    - "What is your relationship to the sender?"
    - "What is the purpose of the transaction?"
- Refuse to payout the transaction and inform the receiver that the transaction is not available at that time.
- Follow procedures to complete an STR, if required.

If the staff determines that a fraud-induced transaction has occurred at the location, or if a consumer submits a complaint to the location stating that they were defrauded, the staff should report the information to the head office.

PROTECTING THE OUTLETS / SUB-AGENTS FROM FRAUD

To tighten security at branch location(s) and to help prevent sub-agent location(s) from becoming a victim of fraud, never perform any of the following actions:

- **NEVER** send a money transfer transaction without first collecting funds.
- **NEVER** enter any information into the money transfer system based on a request from an incoming phone call.
- **NEVER** agree to a personal computer support connection unless you have previously initiated contact with head office regarding an issue with your personal computer, even if the caller states they are from money transfer organization or your network's technical services.
- **NEVER** download software from an unknown source or insert a CD/USB (given to you) into the personal computer that is used to provide software installation services.
- **NEVER** enter a "test" or "training" transaction into the live system.
- Personal Computers with money transfer services should run industry supported software only and must be upgraded/patched in a timely manner when prompted. Ensure adequate anti-virus, anti-spyware and firewall programs — set an auto-update/auto-run for daily protection.
- Do not run non-company email or other software on a personal computer used to process money transfers.
- Set designated hours of operations in the money transfer system so that the money transfer system is not active after normal business hours. Shut down the personal computer after the location's hours of operation.
- Employees should lock personal computers when leaving their work stations.
- Delete all Operator identification documents for any resigned or former staff.
- Operator identification documents and passwords should never be shared with anyone, including other employees or anyone requesting passwords over e-mail or text. System passwords should be changed every 90 days.

EVERYDAY FRAUD PREVENTION PRACTICES

There are common practices that the company shall implemented that will assist in preventing fraud against consumers and against the company own locations. These include:

- Reviewing the Fraud Awareness education materials that Company has provided at location
- Promptly reviewing any fraud alerts from foreign associates that are posted on the money transfer system or in Agent Portal (these messages contain timely fraud alert information)
- Never allow consumers to see the personal computer screen when the staff is entering transaction or consumer information into the system
- Never allow unauthorized persons access behind the counter or near the money transfer transaction area; and
- Never respond to e-mails, phone calls or faxes requesting money transfer computer login/account information, such as account numbers, terminal IDs, operator identification documents and passwords.

IMPORTANT NOTE: Money transfer organization (MTO) will never contact a branch / subagent location to instruct the location staff to complete transactions on the system without obtaining payment, for any reason. System tests are never performed in live system mode. Any such communication you receive is likely an attempt to defraud you and should be reported to compliance department immediately.

FRAUD COMPLAINT MONITORING REPORT (FROM MTO)

The fraud complaint monitoring report is a list of fraud complaints, separated out by send-side and pay-side transactions that have been reported by the MTO. The report is sent each month to the designated compliance point-of-contact (POC)/Manager Compliance and will include all locations in the network. It is the responsibility of Manager Compliance to cascade the report to individual locations as they deem necessary.

Transaction characteristics and patterns will vary by location. Any kind of unusual or uncharacteristic activity against location should be noted and analyzed.

SEND-SIDE AND PAY-SIDE ANALYSES

Consumers who are sending fraudulently induced transactions are typically the victims of fraud, and consumer who are receiving fraudulently induced transactions are typically the perpetrators of fraud (fraudsters).

So, send-side transaction analysis involves examining senders' transactions and looking for patterns to determine what associates should be looking for when executing send money transfers, and pay-side transaction analysis involves examining receivers' transactions and looking for patterns to determine what associates should be looking for when paying out money transfers.

Customers should be guided that they should never send money to an individual they have not met in person and should confirm all emergency situations are real, prior to sending money.

If, at any stage, there is a suspicion that a customer is victim of fraud, compliance department should be notified immediately.

REPORTING PROCEDURES AND ACCOUNTABILITY FOR REPORTING/NON-REPORTING OF FRAUD

FLA: Where FLA suspects that an act of theft, fraud or corrupt conduct is occurring or has occurred, it is the duty of that FLA to report such suspicions to CSC/compliance team at Head Office.

Record the suspicion / Fraud log: Relevant staff must record details of the report including details of when the report was received, and details of all matters raised.

Notify the Compliance Team: All reports of suspected fraud or corrupt conduct must be reported to the Compliance Manager immediately and prior to any investigation of such allegations being undertaken.

REPORTING SUSPICIOUS TRANSACTIONS

Compliance Team verifies the information provided, determines responsibility, identify improvement opportunities, and determine if the matter requires reporting to the appropriate law enforcement agency. This process may include interviewing the individual filing the complaint.

Transaction that is directly or indirectly involve money laundering or terrorist financing or any illegal/fraudulent activity, must be reported to the local law enforcement agency. Also, as per Chapter 07 Exchange Companies Manual, any event of fraud, burglary, loss, F.I.R lodgment by / against the company or its associates i.e. the franchises, payment booths etc. shall be reported to OSED-SBP.

A Suspicious transaction report (STR) must contain a statement describing why the suspicious had been created initially. The report must contain as much detail as possible.

Information about the transactions reported as suspicious must be kept confidential. Customer must not be informed that a STR has been filed.

INVESTIGATION RESPONSIBILITIES AND PROCEDURES

The Compliance Team will establish whether an investigation is required and the process for an appropriate investigation. The investigation process will have a clear plan that will include:

- Preservation of evidence
- Collection of appropriate evidence through interviews, evidence statements, review of records and transactions, etc.
- Analysis of information
- Appropriate consultation as required with Senior Management
- Clear conclusions and action recommendations and responsibilities.

Review of Frauds

A review on frauds/forgeries/burglaries can be presented to the Senior Management. The review shall include the analysis based on nature/ event type category of fraud, area of operations, Nature of severity and Individual involved etc. The Senior Management shall monitor all the cases of frauds/ forgeries/ burglaries in order to:

- Ensure that actions being taken to restraint such incidents in the future.
- Monitor progress of investigations, court cases and recoveries position.
- Review the efficacy of remedial actions taken to prevent recurrence of frauds/ forgeries/ burglaries such as strengthening of internal controls etc.
- Suggest any additional steps/ actions as may be deemed relevant to strengthen preventive measures against frauds/ forgeries/ burglaries.

The review shall cover the following:

- Total number of frauds detected during the year and the amount involved as compared to the previous years.
- Analysis of frauds according to different categories such as Nature/ Event type category of fraud, Business Lines/ Area of operations, Nature of severity and Individual(s) involved etc.
- Region-wise/ province-wise break up of frauds/ forgeries/ burglaries and amount involved.
- Estimated financial loss to the company during the year on account of frauds/ forgeries/ burglaries, amount recovered so far, and provisions made.
- Number of cases (with amounts) where company's staff/employees were involved, and action(s) taken against them.
- Progress report of the outstanding cases of frauds/ forgeries/ burglaries detected during the year.
- Significant controls introduced/ preventive/ punitive steps taken during the year to curb incidents of frauds/ forgeries/ burglaries.

Confidentiality

Great care must be taken in the investigation of suspected indecencies or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way. An employee who discovers or suspects fraudulent activity will contact the compliance department immediately. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the investigations unit or the legal department.

No information concerning the status of an investigation/information will be given out to anyone internally or externally.

The reporting individual should be informed of the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the Departmental head.

NON-PAYMENT CLAIM

SEARCH REQUEST: PROOF OF PAYMENT (POP)

A Search Request (SR) is a request made in case a customer claims non-payment of funds to the beneficiary at destination, following documents must be provided by the customer

- Written Customer Complaint
- Automated Customer Receipt
- Customer ID
- Any other form as per requirement

RECORD RETENTION & INFORMATION MANAGEMENT

Reference: Company's Record Retention Policy