REMIT UNION

ANTI FRAUD POLICY

Table of Contents

Introduction

Remit Union is committed to deter fraudulent transactions through the education of Agent/ Partners and staff to ensure that victims can be identified and assisted quickly.
The Remit Union Anti-Fraud policy/guide is designed to help detect, deter and prevent consumer fraud.

There are two main risks to the money transfer sector in relation to fraud, **Consumer Victim** fraud and **Agent/Partner Victim** fraud. This document will define both of these fraud types, identify common indictors and cover the types of consumer and Agent / Partner victim fraud. Fraud is a growing issue in the payments sector. The 2017 UK fraud indicator estimates that fraud losses in the UK to be around £190 billion a year. Fraud is the most commonly experienced crime in the UK.

These crimes can have devastating effects on victims. Victims may lose all their savings and can be impacted psychologically. Criminals may use the funds stolen to fund illicit activities which damage society such as people smuggling, terrorism and drug trafficking.

Criminals use a wide range of methods to commit fraud with the theft of personal and financial data through social engineering and data breaches as the major contributor to fraud losses in 2018. Fraud against individuals is typically targeted against elderly and vulnerable people. Fraud is increasingly being committed online whereas previously this was mainly committed through phone, post or in person.

The fraud act 2006 came in to effect in 2007 which gave a statutory definition of the offence and defining it in three classes: false representation, failure to disclose information and abuse of position.

Responsibility

In relation to the prevention of fraud, following are the responsibilities of senior management/directors:

Directors

The directors are responsible for establishing and maintaining a sound system of internal control that supports the achievement of fraud policies, aims and objectives.

MLRO

Overall responsibility for managing the risk of fraud has been delegated to the MLRO. Responsibilities include:

- Undertaking a regular review of the fraud risks to ensure that new typologies are updated in the anti-fraud policy.
- Establishing an effective anti-fraud response plan, in proportion to the level of fraud risk identified.
- The design of an effective control environment to prevent fraud.
- Establishing appropriate mechanisms for:
    - Reporting fraud risk issues

- Reporting significant incidents of fraud or attempted fraud to the Board of Director Directors;

- Making sure that all staff are aware of the Anti-Fraud Policy and know what their responsibilities are in relation to combating fraud;
- Ensuring that appropriate anti-fraud training is made available to Directors, staff and Agent / Partners as required; and
- Ensuring that appropriate action is taken to minimise the risk of previous frauds occurring in future.

Management Team

The Management Team is responsible for:

- Ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively;
- Preventing and detecting fraud as far as possible;
- Reviewing the control systems for which they are responsible regularly;
- Ensuring that controls are being complied with and their systems continue to operate effectively;

System Enhancements-Preventing Fraud

To protect consumers from being victims of scams, the consumer when processing a transaction will be presented with a transaction receipt with a fraud warning, he will need to read this warning and sign the receipt. The transaction will be cancelled if the consumer does not read this warning and sign the receipt.

Consumer Victim Fraud

Consumer fraud refers to criminals deceiving consumers, convincing them to transfers funds for a scheme or through social engineering. A number of different types of scams are used by a criminal, the victim believes that he will receive a financial benefit or that they are helping

a relative or a friend. Elderly or vulnerable consumers are typically targeted by fraudsters but anyone could be a victim.

Most common types of consumer fraud are given below:

Rental Property Scam

This type of fraud is usually targeted at foreign students. The avenues used are gumtree and other sites used to advertise property. The fraudster will set up an advertisement for a property with the rental amount well below the market rate (too good to be true), pictures are used for other properties found on the internet. Due to the competitive pricing of the property, the fraudster will receive a number of queries.

If the victim requests to view the property, the fraudster will claim he is out of the country and will request for a deposit to be sent to ensure that he can reserves the property as demand was high. When the money is sent, the fraudster disappears. The property never existed.

Grandparent Scams

A fraudster claiming to be a relative in distress or representing the relative such as a lawyer or law enforcement will contact the victim. The relative of the grandparent claims that she is in trouble and needs their grandparent to send them funds that will be used to pay hospital fees, lawyers' fees or other fictitious expenses.

The victim is advised by the fraudster not to tell anyone, to only inform the grandparent. Calls may be received at night to confuse the victims.

Unexpected Prize and Lottery Scam

This scam involves a request being received to pay a fee in order to claim a prize or winnings from a competition or lottery that has never been entered in to by the victim. The fraudster will contact the victim via mail, telephone, email, text message or through social media claiming that the victim has won a fantastic prize in a competition or sweepstake that the victim does not remember entering.

The prize could be a holiday, electronic equipment such as a laptop or smartphone or an international lottery. A fee is requested by the scammer to release the funds. They will often claim that the fees are for insurance costs, government taxes, bank fees or courier charges. The scammers make money by continually collecting these fees and stalling the payment of winnings. In order to avoid victims from further looking in to this or asking someone about the scam, fraudsters will urge the victim to keep the information confidential and to respond quickly.

Advance Fee Scam

The victim pays a payment in advance for a promise of goods or services such as a loan or a credit card. After the funds are sent by the victim, the goods or services are never received. The victim is contacted by mail, phones, fax or email.

Mystery Shopper Scam

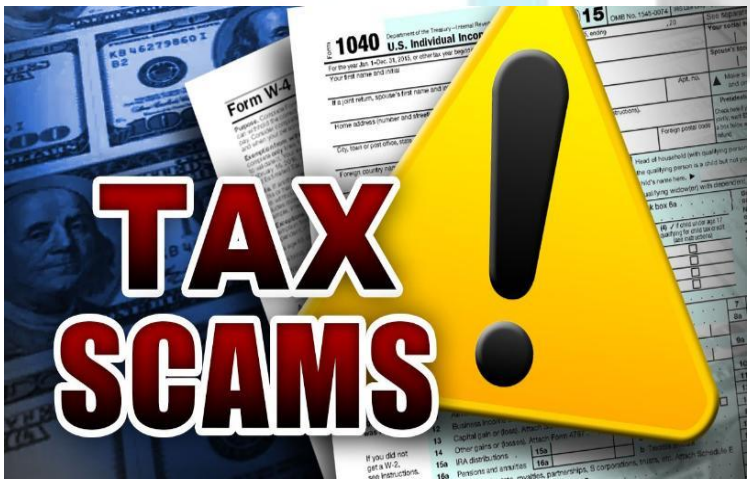
Newspaper ads and emails are used to create an impression that the mystery shopping jobs are a gateway to high paying jobs. Often websites are created where a victim can register to become a mystery shopper but a fee has to be paid to obtain information on

certification programs, to obtain a list of mystery shopping companies or guarantee of a mystery shopping job. The certification offered is worthless, the list of mystery shopping companies can be found for free online and genuine mystery shopper jobs are listed on the internet.

The shopper may also be sent cheques by the fraudster with a request to bank the cheque and to send back an amount. The cheque does not clear and the victim would have sent back a portion of the funds and would be responsible for the bounced cheque.

Employment Scam

Employment sites are used to recruit victims. The victim believes he has an applied for a genuine job. The fraudster then sends a cheque requesting the applicant to bank this to cover the expenses of the credit check, application fees or recruitment costs.
The fraudster will request the victim to use the funds for these expenses which will be required for the job and to send the remaining balance back. The cheque will bounce and the victim will be responsible for the amount of the cheque.



Tax Scam

The fraudster will contact the victim demanding a tax payment, threatening the victim with an arrest, fines, deportation, ceasing of property etc.

The victim will be required to make an urgent payment through a money transfer service provider to avoid the action being by the

government agency. This is not how government agencies operate, tax demands are always sent through the post.

Relationship/Romance Scams

Victims are targeted through online dating apps or social networking sites. Romance scammers create fake profiles on dating sites or contact targets through popular social media sites like Facebook, Instagram etc. The scammers will socially engineer the victims, striking a relationship with their targets to build their trust, this can sometimes go on for months. The scammer will eventually make up a story and ask for money.

Common stories are: working in the military, working as a doctor, requesting for payment for surgery or emergencies, paying off debts & paying for travel or a visa. The victim is requested to send a money transfer. The victim at this point may have become so emotionally involved that it may become difficult to deter them from sending money. Ask the victim to talk to a friend or relative about the situation and refuse the transaction.

Tech Support Scams

Scammers will usually contact the victim either through phone calls or through pop ups on the web browser. When phoning, the scammer will claim he is calling from a well know tech company such as Microsoft and will inform the victim that they have an issue with their pc such as a virus. They often ask for remote assistance and will demand payment via a money transfer service provider for a problem that never existed.

The pop up on the victim system will claim there is a system error or virus issue and request a call to a number where the again the scammer will demand payment for a non-existent issue. Scammers may also try to get their website to show up on online search results for tech support.

Charity Fraud

The victim is contacted by a fake charity or someone claiming to represent a genuine charity with a request for payment through a money transfer company. Recurrent payments may be requested. Genuine charities do not request for payment to be made via a money transfer service provider. Victim may be contacted by phone, email or post.

Family Emergency Scam

Fraudsters will pose as relatives or friends, claiming that they have an emergency and require for funds to be sent urgently.

Common scenarios used: to pay for hospital treatment or to leave a foreign country. The scammer will gather information on the victim from social networking sites or may hack the email of the victim and obtain information on contacts or hack the email of a relative.

They may also involve other crooks that claim to be police officers or lawyers.

Immigration Scams

A scammer will claim to be a government official when contacting the victim and have access to private information on the individual which he will use to convince the victim that the request is genuine. The scammer will then demand payment for resolving any immigration issues that the victim may declare.

The victim me be threatened with legal action or deportation if he does not comply. Immigration officers do not collect money or payments by phone or through money transfer service providers.

Internet Purchases

The victim purchases an item on the internet but the item is not received after payment is made. The items being sold could be well below their market value & may appear to be genuine with the fraudster using various methods to make the item being sold appear genuine.

Fake/Fraudulent Cheques

Fraudster will send a cheque for an amount more than what the victim expects to receive for a product or service. The fraudster will request to bank the cheque and send back the excess amount through a money transfer service provider.

The cheque will bounce and the victim will be left out of pocket. As described earlier, the victim may also be sent a cheque to cover the expenses for accepting an employment, purchases etc. & will be left out of pocket when the cheque bounces.

Telemarketing

This refers to the marketing of goods and services by telephone, usually unsolicited to potential customers. This covers a number of different fraud types where consumers are contacted by phone e.g. charity fraud, lottery scam, internet purchases, immigration scam & advance fee scam.

Preventing Consumer Fraud

The most important indicator that a consumer may be a victim of a scam is that they would not have met the receiver. Usually social engineering can last for months/ years and the criminal will not ask for money initially. The aim is to build trust and have the victim emotionally involved at which stage the criminal will ask for money. It is important to familiarize yourself with the various scam types which are discussed later in this document so that victim can be identified and helped quickly.

Common red flags indicating consumer fraud:

- Consumer has found a once in a lifetime deal, seems excited
- Consumer may not have sent previously, enquires about the process for sending money
- Consumer may indicate that they money is being sent to resolve an urgent emergency
- Consumer may not be able to provide info on source or purpose
- Elderly or vulnerable consumers sending to unrelated individuals
- Consumers sending a number of transactions in a single day or over a number of days
- Change in sending pattern if sent previously

If suspicions are raised in relation to a consumer being a victim of fraud, investigate further:

- Inquire from the consumer if they have met the receiver
- Ask the consumer about his relationship with the receiver
- Can the consumer provide information on the purpose of the transaction, does the consumer appear confused?
- Does the consumer become emotional when probed further?
- If the consumer indicates that he has received an email from a relative who has an emergency, request the consumer to call the relative and confirm

Take the following action if you suspect that a consumer may be a victim of fraud:

- Refuse the transaction
- Inform the consumer that this transaction may be linked to a scam, call the Remit Union head office for support in advising the consumer
- Report the incident to the Remit Union head office
- If a vulnerable consumer is at risk, submit a SAR

Differentiating between victims and fraudsters:

A number of scenarios have been provided in relation to consumers that may be victims of fraud but a fraudster may also visit a location to collect funds. Common signs to indicate that the consumer may be a fraudster:

- The ID being used appears suspicious/ fake
- One to many transactions received by the fraudster
- No relationship between the sender and receiver
- Consumer may be reading from a phone, has a list of control numbers

If there is suspicion that a fraudster is at a location, the transaction must be refused, Remit Union will need to be informed immediately so that the transaction can be blocked. A SAR will need to be submitted.

Agent / Partner Victim Fraud

Agent / Partner victim fraud is defined as deceptive and fraudulent business practices that cause Agent / Partners to suffer financial losses. An Agent / Partner can be targeted in a number of different ways. Some of the most common ways in which an Agent / Partner can be targeted are given below:

Hijacking of PC

Hijack refers to taking control of a pc through malware and trojans. The victim may visit a malicious site where software is downloaded inadvertently or malicious software is unknowingly downloaded through an email, by clicking on an attachment. Using keyloggers, the hacker is able to record personal information such as passwords. This can compromise the username and passwords of an Agent / Partner.

Requesting Remote Access

A fraudster can call claiming to be from Remit Union and requesting remote access to help with an issue or to conduct an update, username and password of the Agent / Partner will be requested. Common PC remote access software may be requested to be downloaded such as team viewer. The fraudster could also ask the victim to turn off the pc while he works on the pc. The fraudster will then conduct a number of transactions. The Agent / Partner will only

realise that the transactions have taken place when he reconciles the banking by which time the transaction will have been paid.

Conducting a Test Transaction

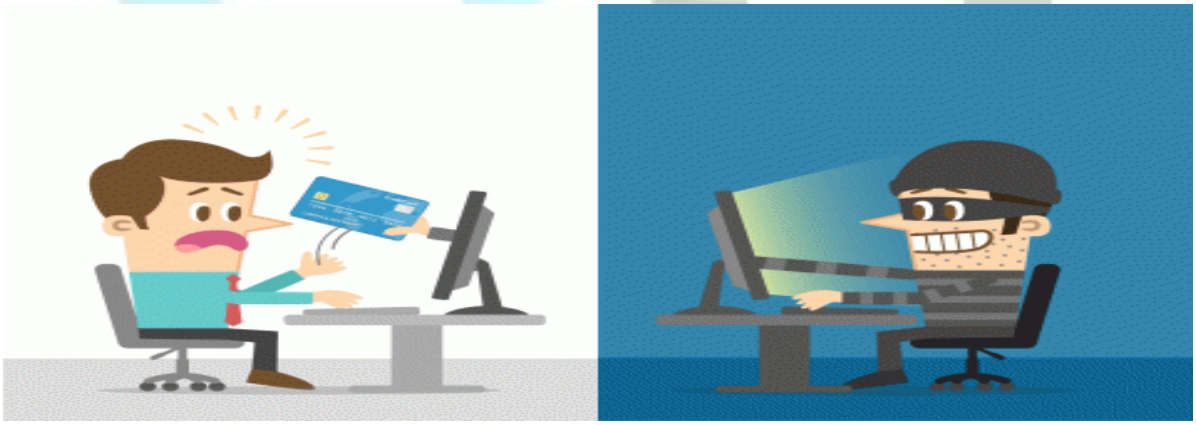
Agent / Partner receives a call from someone claiming to be from Remit Union , the Agent / Partner/operator is requested to conduct test transactions but the transactions are actually real and are paid out.

Phishing Pages

A hacker will send a login page of Gmail, Facebook, PayPal etc which looks exactly the same as the real Facebook or Gmail login page. The link can be sent through text or email. The victim may not realise that his password has been stolen. This can also be used to propagate malicious software to a computer & gather personal information on the victim.

Phone Spoofing/ Phone Hijacking

Fraudsters hijack or imitate phone numbers, either to imitate a person, business or department to get money or information. Or to appear like a local or legitimate number to increase their chances of getting through to their victim. Even if the fraudster claims he is calling from Remit Union and the number being called from appears genuine, it could still be a scam. Crooks are using phone hacking and hijacking to conceal their identities during phishing scams.



Underpayment

A consumer comes in to process a transaction, may look for busy times so as the Agent / Partner is distracted. The fraudster is looking for the transaction to be processed before the funds are checked. He may leave the money on the counter while the transaction is processed.

When the transaction has been processed and the Agent / Partner checks the money, he finds that it is short. The fraudster will request to visit an ATM to withdraw the money but will not return. The recipient will be looking to collect the funds quickly to avoid the transaction being cancelled. Even if the payment number has not been provided, if the pc screen is visible, the fraudster may have noted this down.

Preventing Agent / Partner Victim Fraud

The following measures can be taken to prevent Agent / Partner victim fraud:

- Installing a firewall and an anti-virus program. Ensuring that they anti-virus software is regularly updated.
- For suspicious emails, hovering the mouse over the email address will provide details on the intended recipient e.g. an email from Remit Union may show as Remit Union when viewing the email but when the mouse is hovered over the address, what is shown is completely different. Delete this email.
- Hovering the mouse over suspicious links, again this will show where the link is directed.
- Remit Union will **Never** request the username or password of an Agent / Partner or request remote access unless a complaint has already been logged. If such a request is received, no information should be provided which will allow the fraudster to have access to the system.
- Agent / Partner should be extremely wary of emails that have generic greetings, unsolicited correspondence, requests for personal information, have bad grammar or spellings.
- Agent / Partner should **Never** process a transaction until the funds have been checked.
- Agent / Partner should **Never** accept a request to access the pc or give out the username of password
- **Never** accept a USB or CD with consumer details or for installing software.
- If the caller provides a number to call, **Never** call this number.
- Agent / Partner should **Never** leave the PC without first locking it.
- If an operator leaves, the log in codes should de-registered asap.
- Operator ID's and password must never be shared.
- Keep the computer screen hidden from consumers, Agent / Partner should **Never** have this consumer facing.
- Unauthorized individuals should not be allowed behind the counter.

Reporting of fraud

All fraudulent activity identified will be reported by Remit Union to action fraud: https://reporting.actionfraud.police.uk/login

For vulnerable consumers or where there is a suspicion that a fraudster may be collecting funds in the UK, this will also be reported to the NCA.