Anti- Fraud Guide

Contents:

Introduction

The purpose of this Anti-Fraud Manual is to raise awareness about the modus operandi used by fraudsters against our money transfer system. This manual is addressing Unitylink Financial Services Group ("Unitylink") employees, agents and online customers.

Managing fraud risks is a key objective for Unitylink. Firstly, there is the obligation to protect our system from becoming an instrument for fraudulent activities and there is the obligation to warn our customers for such activities. Secondly, Unitylink wants to protect its reputation as a reliable money transfer services. Our company will take action against any form of criminal activity, whether it is money laundering, the financing of terrorism, or fraud.

In this manual, we provide you details about potential fraud schemes. Practical examples of how fraudsters operate will be also discussed. Finally, we will give you some important tips to secure anyone using the Unitylink system from becoming a fraud victim.

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.

Fraudulent Abuse of Money Transfers

Fraud related to money transfers is committed against two different victims:

1. Our customers who transfer money to a fraudulent beneficiary
2. Employees or agents working for Unitylink

The first group, our customers, is the most targeted victim. Customers can become the victim of various schemes used by fraudsters to illegally appropriate money from the customer or to steal money from others through the customer. But also you, the person operating the Unitylink system to conduct orders for our customers, can be the victim of fraud. In this case, fraudsters try to access to the money transfer system abusing your system password. In the next section of this manual you will find some case studies that discuss different types of fraud schemes.

Customer-focused money transfer fraud:

By telling a credible story, fraudsters motivate their victims to transfer money to unknown and unreliable beneficiaries.

Agent-focused money transfer fraud:

By gaining unauthorized access to REMIT1 money transfer system, fraudsters initiate orders at the financial expense of victimized agents.

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.

Fraud Examples

In this section we will discuss the characteristics of money transfer fraud. General examples of fraud are:

1. Internet or auction purchases
2. Taxes or other fees to claim lottery prize winnings
3. Down payments or fees to loans
4. Investment opportunities
5. Emergency situations with someone you have met on-line
6. Jobs that can be done from home, but that need a fee for training

Apart from these examples – of course – other types of money transfer fraud exist and new types emerge regularly. But, generally they have similar characteristics you can learn to recognize. Below we will discuss some types of fraud more in detail, to give you a good idea what kind of characteristics to look after.

Loan Scams

Criminals are always looking for new ways to steal money from innocent victims. One ways they accomplish this is by convincing your customer (hereinafter referred to as "victim") to send them money by using our money transfer service. The criminal uses clever techniques to defraud the victim. These criminals target those who are down on their luck, those that have recently lost their job, or those that are struggling to meet financial obligations during this tough economy. In the following example, the criminal presents themselves as a loan officer (hereinafter referred to as "criminal") for a bank or other financial institution and focuses on those individuals that are in need of a much-needed loan. This individual contacts the victim via telephone, e-mail, or by traditional mail and explains that they have been pre-qualified to receive a loan of up to € 5,000. The criminal offers low interest, low monthly payments, and approves the loan with little or no credit check. Even though the victim might be skeptical at first, the criminal assures the victim with certainty that they will receive the loan within a one-week period. As a show of good faith, the criminal instructs the victim to use our money transfer service to pay for the first five months of the loan. The victim agrees to pay € 1,000 up-front for the loan (€ 200 per month, times 5 months, is € 1,000). At the end of the week, the victim realizes that the loan has not been deposited into their bank account. The victim then tries to contact the criminal, but realizes that the phone number is no longer in service. The victim then sends an email to the criminal, but receives no response.

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.

The victim's last option is to cancel the transaction and receive a full refund. The victim, however, is ineligible to receive a refund because by then the criminal has already picked up the money. This so-called loan scam is designed to steal your money.

Rogue Traders

Rogue traders (or "bogus callers") call uninvited at people's homes impersonating as a legitimate business or trade. They are often members of mobile and highly organized crime groups and travel the country seeking areas with a high population of older residents or mixed communities. They are known to share information about suitable areas for criminal exploitation with other criminals. They deliberately overcharge for unsatisfactory or unnecessary work, damaging property purposely to obtain the work, leaving work unfinished, and using aggressive and intimidating behavior to extort money. Rogue traders place extreme pressure on vulnerable people to obtain money, sometimes accompanying them to financial institutions to withdraw cash, and often extort money from the victim over a protracted period. Many older people become increasingly isolated following the loss of a partner and their garden and exterior house maintenance may indicate their vulnerability, making them more susceptible to exploitation by criminals.

Sidi Salem Fraud

This type of fraud mainly originated in Tunisia, but has now spread to several European countries such as France, Italy, Germany and Belgium. The name "Sidi Salem" fraud refers to people in Tunisia selling wine. The same method is also used in other forms similar to Nigerian fraud. It is claimed that the person involved has won a suitcase filled with money and is requested to pay customs clearance charges or legal fees for this money. The fraudsters will try to reach as many potential victims as possible, mainly by phone. They sell high-quality wine at excessive prices compared to the European market price. Due to the high price the victims initially respond that they are not interested, the victims are then phoned repeatedly, sometimes several times a day. Most victims are elderly people, they prefer to give in and accept the offer so the harassment would stop. Large amounts of money are involved in the transactions, sometimes even tens of thousands of Euros in a few months' time. Moreover, the victims who actually receive the wine agree that it is simple table-wine.

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.

Advanced-Fee Schemes

In an advanced fee scheme the victim pays money to a fraudster in anticipation of receiving something of greater value e.g. a loan, contract, investment, gift etc. They then receive little or nothing in return. This scheme also involves such things as the sale of products or services, holidays, prizes, investment offers and lottery winnings.

Nigerian Fraud

The offenders first try to contact potential victims on a large scale through the Internet or e-mail. The victims get a lucrative offer; this may be a contract, a winning lottery ticket or inheritance that can be claimed. In case of a “romance scam” pictures of handsome men and women taken from the Internet are advertised on dating sites or forums. In case the victim reacts to this first proposal personal information is requested from the victim and additional documents are sent to make the offer more credible. Shortly afterwards the customers are requested to send an advance in order to claim the entire amount, or the “Internet date” suddenly turns out be in need of money. The requests for money continue until the victims get suspicious and stop paying. The money for Nigerian fraud will generally be sent from North America, Western Europe or the Arabian Peninsula to various countries in West Africa. Especially Nigeria, Côte d’Ivoire, Senegal, Togo, Ghana and Benin are common as a final destination of the money. However, fraudsters increasingly use intermediaries in Western Europe to receive the money and send it on to West Africa. This puts up an additional barrier between the offender and the victim. When these intermediaries are established in Europe the transactions may be split up in funds received from principals in other Western countries on the one hand and transfers to beneficiaries in West Africa on the other.

Lottery Schemes

Lottery schemes involve victims receiving emails or letters promising huge winnings, invariably from an overseas lottery that claims the victim has been allocated winning numbers. The victim is asked to contact the organizers and send money to cover the administration costs to release the winnings – which do not exist.

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.

Money Mules

The money mules phenomenon can be described as follows. Criminal organizations try to lure people through employment advertisements on the Internet. Those who agree to this are usually unemployed or young people. They have to grant access to their bank account to which money is transferred, usually from abroad. The account holder then has to withdraw the money in cash fairly shortly after receiving the money and transfer it abroad using a money transfer agency. The individuals involved can keep 10% of the deposited money as a commission. The employment contracts sent by e-mail look very professional and complete. The companies seem to be genuine ones wanting to offer people the chance to earn some additional income. It is striking that Russian companies are often involved as potential employers. The funds transferred to the account are often the proceeds of a "phishing" scam, which is a scam on the Internet. People are lured to a fake banking website and asked to enter personal banking details. As such fraudsters can obtain credit card numbers to withdraw money from the accounts without the victims' knowledge. These are usually accounts with German, Belgian and Danish banks.

Share Sale Fraud

Share sale (or "boiler room") fraud sees the victim receive unsolicited phone calls or correspondence concerning investment matters. These are typically from overseas based "brokers" who target European shareholders, offering to sell them what often turn out to be worthless or high risk shares in US or UK investments. The "brokers" can be very persistent and extremely persuasive.

Used Car Offers

This particular scam begins with an advertisement on a website or motor magazine, where e.g. an English seller is trying to sell a top-of-the-range car at a knock-down price. The seller usually says he is abroad in a country like Spain or Portugal, and needs to sell the car quickly. They tell victims they are unable to see the car as it's already with a shipping company. In fact, there is no car and victims have already parted with their cash by the time they realize this is a scam.

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.

Tips for Customers

In this final section, we provide you with some important tips in order to stop fraudsters. Observing these tips will significantly reduce the risk of becoming a fraud victim.

Tips for customers to stop fraudsters:

- Never send money to someone you do not personally know.
- Never send money first in order to get something in return later on, like for a lottery, a job, or a loan.
- Do not believe an emergency story from someone who says to be a relative without verifying the person really is your relative.
- Do not believe in offers that state a money transfer is the only possible way of payment.
- Think before you act, an offer that sounds too good to be true is usually too good to be true.
- There is no protection against loss due to a fraudulent money transfer as it is similar to sending cash.

Reporting Fraud

If you believe you discovered an attempted or a case of fraud, please immediately report it to us to the below contact details . You can contact us internationally in the following ways:

Telephone: +44 (0) 208 772 2160
Fax: +44 (0) 208 675 3716
E-mail: info@unitylink.com

Information in this document is confidential.
It is intended solely for the person to whom it is addressed, and must not be used or copied by any other person.