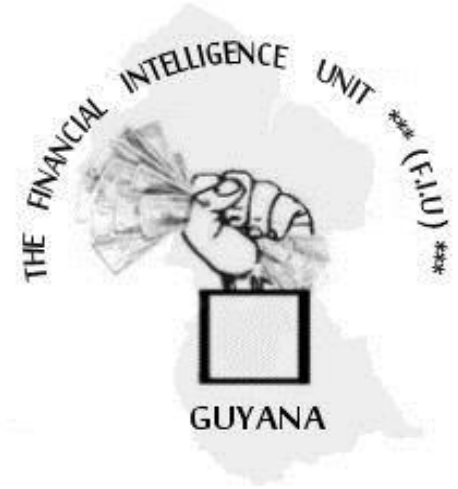
FINANCIAL INTELLIGENCE UNIT



WIRE TRANSFER FRAUD TYPOLOGY 2016 - 2018

Table of Contents

.

DEFINITION OF KEY TERMS AND ABBREVIATIONS

Beneficiary Bank: The bank wherein an account in the name of beneficiary or payee is held.

Browsers: Programs or software that are used to access information on the World Wide Web.

Call Back Contact: This refers to the person identified in an institution to whom verification or confirmation phone calls should be made.

Data Encryption: This refers to the translation of data into another form or code thus allowing only authorized users with a password to access same.

Domain: This refers to an entity's unique name on the internet.

Hacking: The malicious and unauthorized intrusion into computer systems or networks.

Malware: This is the abbreviated term for 'malicious software' and it refers to programs that are designed to infiltrate and damage computer systems.

ML: The abbreviation for "money laundering" which is the act(s) of concealing or camouflaging the true source(s) of illegally obtained money thus making such funds appear legitimate.

Phishing: The use of fraudulent email addresses and/or websites to solicit personal and sensitive information from an individual or company by pretending via electronic communication to be a trustworthy individual or entity with whom or which the former is familiar.

Spoofing: This is where an electronic communication, using a forged email header, is fraudulently or maliciously sent from an unknown source, disguised as a source familiar to the receiver.

TF: The abbreviation for 'terrorist financing' which means the provision of funds for terrorist activity.

Transactions: In the context of this report, this refers to the transfer of funds from the customer's bank account to the supplier's bank account.

URL: The abbreviation for Uniform Resource Locator which means the address of a webpage or file on the internet.

Wire Transfer: This is a form of electronic transfer of funds from one individual or entity to another. Such transfers can be made from one bank account to another or from one bank to another. The remitter may or may not be in the same country as the receiver or beneficiary.

INTRODUCTION

This typology seeks to highlight some of the means by which individuals infiltrate the email/network systems of organizations by impersonating key officials in the payment process, to fraudulently obtain financial benefits. Because these types of frauds often transcend international boundaries it is very difficult and sometimes too complexed and costly for companies to pursue recovery of funds lost due to these fraudulent activities.

Phishing and spoofing are two of fraudsters' primary tools to obtain sensitive information from potential victims (individuals and companies alike). The perpetrators of these frauds aim to illegally obtain funds by intercepting the chain of emails of their victims, their victims' suppliers and/or customers and manipulating, misrepresenting, modifying or falsifying payment details and instructions to redirect funds to themselves. The losses associated with these types of frauds are significant and can potentially impact the viability of some businesses.

It is therefore very important that organizations be aware of the potential risks of this type of fraud and adopt mitigating measures to safeguard their entities from significant losses. This may also result in their organizations being unknowingly linked to money laundering and terrorist financing activities.

The Anti-Money Laundering and Countering the Financing of Terrorism (AMLCFT) Act 2009 specifically lists, in the Second Schedule, the offence of "fraud" among the serious or predicate offences that are linked to money laundering or terrorist financing.

The mission of the Financial Intelligence Unit (FIU) is to, among other things, aid in the detection, prevention and deterrence of money laundering, terrorist financing or proceeds of crime. By way of this typology, the FIU seeks to bring awareness to reporting entities, supervisory authorities, competent authorities and the public, to the potential ML/TF risks that are possible through cyber frauds committed via computer network systems.

This typology also seeks to provide recommendations that may be considered by the target audience, in the formulation of policies, procedures and controls, to ensure protection of their systems from criminal enterprises.

TYPOLOGY

It has been observed with great concern that there has been an increase in the incidence of and attempts to commit the fraudulent transfer of funds using wire payments at commercial banks. These acts have been noted to be targeting a number of larger business enterprises in Guyana.

The perpetrators have been using what seems to be advanced internet and computing technology to intercept emails of senior officials who are responsible for approving payments by their respective companies. The aim is to impersonate the company's officer in order to extort large sums of money by way of fraudulent wire transfer requests. The email account interception/ hack allows the scammers/fraudsters, once undetected in a timely manner, to monitor and/ or manipulate the emails of the senior company official. This allows the hackers to observe the nature and details of communications with customers, suppliers and financial institutions. This includes the key contacts, transfer trends, and other details relating to the facilitation of payments by the company to the supplier via a financial institution. With this information, the perpetrators then proceed to dispatch fraudulent e-mails representing themselves to be:

(i) the suppliers' contact persons requesting payment for goods while at the same time issuing amended banking details for such remittances; and
(ii) the senior officials of the local businesses (customers) instructing financial institutions to wire transfer such payments in accordance with those amended banking details.

Spoofing and Phishing are usually the manner by which the fraudsters gain entry into the networks of these entities i.e. cloning company letterheads, signature blocks and logo so as to "spoof" or trick the recipients into thinking it originated from a legitimate source. This allows them to gain the trust of the receiver (usually the paying company and/ or the financial institution) to follow the revised instructions or a link which will enable the divulgence of key user information, i.e. "phishing". Phishers are effective at impersonating individuals, by creating email addresses almost identical to the legitimate ones, for example: by interchanging or modifying two letters or adding an extra letter in an email address. The perpetrators press for the fraudulent transaction to be completed in the shortest possible time, to avoid detection before the payment is remitted by the financial institution.

The aim of this attack is to trick the email recipient into believing they are dealing with their usual/ a trusted entity. The change in e-mail address is intended to be of such miniscule proportion that only very careful reviewers and/ or automated systems may immediately detect the change.

SUCCESSFUL WIRE TRANSFER FRAUDS:

Case 1:

A Finance Manager, in responding to an email sent by someone impersonating a known contact person at one of its suppliers, disclosed information such as names and account numbers of both their and the supplier's banks. Two weeks later, another email from an individual once again purporting to be the supplier's contact person was received, indicating that payments were overdue, but should be made to a different bank account.

Subsequently, the company performed its usual verification procedures for wire transfer payments, the instructions were sent to the bank and the payment was effected based on the revised (fraudulent) instructions.

The Managers were unaware that the emails were sent by scammers. A bona fide representative of a supplier, shortly after wire transfer instructions had been issued to the bank, notified the payer that no such payment request was made, and that the revised banking information was not authentic nor was it provided by the company's representative. The paying company contacted the financial institution and attempted to recall the transactions. They were however unsuccessful as the overseas "beneficiary bank" advised that the beneficiary customer had already withdrawn the funds and closed the account.

Due to this phishing attack, the company suffered a financial loss totaling over US$480,000 This was despite having an operational policy requiring that all banking instructions sent by clients/ suppliers via email for payment, must be verified by a phone call and further confirmed by fax. In this case the policy and controls were not fully and strictly followed.

Case 2:

A fraudster hacked into the e-mail account of an employee of a major supplier for a large international company/ importer. An email prepared by the hacker, based on information availed from the employee's email history, requested payment using modified banking details. Two days later the requested sum of over USD $250,000. was wired to the fraudulent account. Two months later, another payment for a similar amount was requested and was also wired to the same account in accordance with the modified banking instructions. The fraud was discovered after the paying company requested a statement of accounts from that supplier, to fulfil a request by its external auditors. It was discovered that the bona fide supplier had never requested nor received the two wire transfer payments in question. Investigation of same revealed that the payments had instead been made to the accounts of fraudsters, following a breach of the supplier's email system.

UNSUCCESSFUL WIRE TRANSFER FRAUD ATTEMPTS:

In other cases, even though senior company officials were unsuspecting, the vigilance of bank officials prevented wire transfer frauds from being committed.

Case 1:

In one such case, a bank representative received instructions via email from someone representing themselves to be a senior official of one of its corporate customers, which is a well-established large manufacturing and retail company. The email requested that over USD $200,000 be wired to an overseas supplier. Vigilant bank officials realized that neither the beneficiary nor the amount requested was in keeping with the established/ documented profile of their customer i.e. the local company. The bank contacted the bona fide official of the local company who advised that they had no knowledge of the transaction and confirmed that they did not issue instructions to the bank in that regard. The bank therefore realized that this was a fraudulent wire transfer attempt.

Case 2:

A commercial bank received an email from someone purporting to be the "Call Back Contact" for one of its overseas-based customers. The email instructed the bank to wire transfer over USD$ 50,000 from the company's account to an overseas beneficiary. The bank officials realized that the beneficiary and the requested sum were not in keeping with that customer's profile. The bank also discovered that the email address, contact telephone number and signature on the wire transfer form were different from what were known to the bank. The bank proceeded to contact the bona fide Client Call Back Contact and received confirmation that the customer did not issue those wire transfer instructions. Hence the bank was able to conclude that this was a fraudulent wire transfer attempt and thus refrained from effecting the transfer.

Common features of attempted and successful wire transfer fraud cases:

- Interception or hacking of e-mail messages of senior company officials with the aim of obtaining information on suppliers, customers, orders and payments, which is subsequently used to impersonate the said officials. System audits revealed that the email accounts in both of the successful cases had been compromised at least two days prior to the receipt of fraudulent emails containing amended banking instructions.
- Instructions may be sent from the same email address or one that is almost identical to the legitimate address of the bona fide company official, requesting the fraudulent wire transfers.
- Invoices and official company documents, including logos, letterheads and signatures are forged causing documents to appear legitimate.
- Repeated and very persistent follow up requests for payments to be expedited (rush/ urgent) are made by scammers via email or even telephone.
- Notification of new bank account/banking details are sent by the impersonators/fraudsters. The scammers may claim that the usual bank accounts are under "Audit and Reconciliation ", hence the need for payments to be sent to the new bank accounts.
- Fraudsters usually provide revised banking details, preferring to use banks in jurisdictions where they perceive the funds will be difficult to recover.
- Weaknesses in the internal control and information technology systems of the paying or payee companies are usually the source of the breach that is exploited by the fraudsters.
- The vigilance of local bank officials can assist in some attempted wire transfer frauds being detected/ prevented.

RECOMMENDATIONS FOR FINANCIAL INSTITUTIONS

- Financial Institutions should institute multi-level verification methods to confirm the identity of person(s)/organization's representatives who provide instructions to effect wire transfer payments via email or any other non-personal method.
- Banks should establish clear profiles for customers' wire transfer activities (amounts/ authority limits, beneficiaries, regularity, Beneficiary Bank details, etc.), so as to hopefully identify unusual or fraudulent requests.
- All changes to normal customer instructions should be appropriately verified, and if necessary, the customer profile updated.
- Banks should advise customers to always check the detailed spelling of the URLs in email links before clicking or entering sensitive information, especially those relating to requests to execute wire transfer payments.
- Banks should implement an appropriate customer call-back system for all wire transfer transactions requested via e-mail or any other non-personal means.
- Banks should sensitize customers on the risks of using non-personal methods of requesting wire transfer payments and best practices to safeguard against wire fraud.

OTHER CONSIDERATIONS

- Watch out for URL redirects; do not provide information where you appear to have been subtly redirected to a different website with identical design.
- If a suspicious e-mail is received from what appears to be a known customer or customer representative, the sender should be immediately contacted via telephone or some other direct manner to verify the email.
- Always pay close attention to the email sender's display name. Most companies use a single domain for their URL's and emails; therefore, a message that originates from a different domain should be seen as a red flag and investigated for authenticity.
- Use of data encryption and protection for file attachments are recommended when sharing financial details and account information via email.
- Secure browsers and email accounts against phishing and malware using appropriate spam and web filters.
- Conduct scheduled anti-virus updates to protect IT systems from external attacks by fraudsters.
- Establish an appropriate customer call-back system to confirm transfer requests in general and changes to usual details including but not limited to beneficiary bank information.
- Careful attention should be paid to the text of email communications. Scammers tend to make grammatical and spelling errors, since there is a possibility the scammers are from a country that speak a different language.
- Provide training to employees on how to detect and deal with phishing, email spoofing and other cyber related security risks/ threats.

DIRECTOR

FINANCIAL INTELLIGENCE UNIT - GUYANA