International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Money Mules on the Rise in India As E-Fraud Thrives Through Social Media

Dr. M. Ruben Anto & Juvitha Varghese
Assistant Professor AMET Business School Academy for Maritime Education & Training (AMET) Kanathur, Chennai – 603 112

e-mail : rubenantonick@gmail.com

PhD Research Scholar Department of Commerce University of Madras Chennai – 600005

Email: juvitha@gmail.com

ABSTRACT
Digitalization and globalization ensure that national and international crime over the internet gets easier and becomes more widespread. Even tactics about performing a crime are being spread throughout the Internet. Social media has taken the world through dozens of websites, mobile apps, and other forms of technologies. This article focuses on the rise of money mules through social media which is an important issue in cybercrime.Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement. A money mule is someone recruited by criminals to transfer the profits of their illegal activities.
Key words: Money Mule, Digital Money, Digital Banking, Cybercrime, e-Fraud

INTRODUCTION

People nowadays are dependent on the use of computers, as they are improving the way they communicate with each other and having a social life and the way they conduct business is different from the old times. Digitalization and globalization ensure that national and international crime over the internet gets easier and becomes more widespread. Even tactics about performing a crime are being spread throughout the Internet. Social media has taken the world through dozens of websites, mobile apps, and other forms of technologies. There are social media sites that have millions of members allowing them to share photos, videos, text messages, and more on a regular basis. Now world has turned into a scenario where people cannot live without social media like Facebook, twitter, LinkedIn, etc.

This article focuses on the rise of money mules through social media which is an important issue in cybercrime.**Money Mule** is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement. A money mule is someone recruited by criminals to transfer the profits of their illegal activities. The money may have been stolen directly from another bank account or may be the profits of fraud, drug trafficking, child Labour or prostitution. Most of the criminals carrying out this type of crime are located abroad, so a money mule based in the UK is required to transfer the money overseas. Although some money mules know that they are handling stolen money, criminals also target groups such as university students to unwittingly laundering the funds on their behalf. In a depressed job market people started looking jobs in online and finally they could be hired as 'money mules', often without knowing its implications, and end up behind bars. A cyber police explains the situation in a money mule case as: An online job-seeker

comes across a foreign 'company' which pretends it has clients in India, and wants to hire an India branch manager to take care of collections. Following an online interview, the job seeker is appointed, with the brief to transfer money that is deposited into his personal account by the company's 'clients', to the headquarter abroad, keeping a 10% commission. The appointee is also promised a monthly salary. What he doesn't know, however, is that he has just been made a money mule.

How do fraudsters operate?

STEP 1: Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

STEP 2: The fraudsters then transfer the illegal money into the money mule's account.

STEP 3: The money mule is then directed to transfer the money to another money mule's account - starting a chain that ultimately results in the money getting transferred to the fraudster's account.

STEP 4: When such frauds are reported, the money mule becomes the target of police investigations.

OBJECTIVES

The main objectives of this study are :

1. To study the impact of social media on the rise of money mules in India.
2. To determine whether people are aware of the e-fraud in social media.
3. To find out the awareness of prevention measures of money mules in India.

SIGNIFICANCE OF THE STUDY

The purpose of this paper is to find out the impact of social media on the rise of money mules in India and to let more people to understand the concept money mule and the consequences of being a money mule. This article also focuses on the cases related to money mules in India and its effectives measures to reduce e-fraud through social media in India.

METHODOLOGY

A qualitative methodology approach was used with the purpose of allowing the research to capture an in-depth understanding of money mules in India. An in-depth interview with the purposive samplingwas madefrom 14people working at LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs, Govt.of India, who had at least five years of experience in studies and research in e -fraud. The similar methodology was adopted in collecting data from IG for the Kannur range, Tomin JThachankary which helped in the research study to find out the impact on people who fall into e-fraud. The purpose of interview with them is to find out more cases of e-fraud in the current era and the consequences of being a money mule. Some suggestions were taken from eminent people working in this field to reduce the e-fraud in India.

MAJOR FINDINGS OF THE STUDY

The e-fraud involves deceiving other people on the net, getting them to part with money, either through the tried and tested lottery-win trick, or by asking for advance money for a visa processing for a job, or something similar. The victim is given the bank account number of the money mule, and asked to deposit money into that account. As soon as that is done, the mule

sends 90% to the fraudster abroad, which completes a round of international rip off, that leaves two Indian nationals in deep trouble - the mule for being involved in the act, even if unwittingly, and the other in financial crisis. IG for the Kannur range, Tomin J Thachankary, who also heads the cyber cell in Kerala, says online frauds have been on the rise, and that many of these have their origin in Nigeria. Thachankary's team in Kerala had arrested two Nigerian nationals late last year, one of who is still in custody, after an elaborate investigation that involved the efforts of police officials of Maharashtra, Karnataka, Tamil Nadu, Andhra Pradesh and Puducherry.

"What the mules don't know is that they too can be implicated as the investigation proceeds", says cybercrimes specialist ES Bijumon, a circle inspector attached to the cyber cell. Money mules, who are initially elated when they get to keep 10% of funds that come into their personal account from unknown sources, realize they are in trouble once police catch up with them after a victim complains. Bijumon says some mules even opt to get out of legal trouble by offering to pay out of their own pockets to those who deposited money into their accounts. Incybercrime investigations, police have tracked the fraudsters to Nigeria in many cases. So much so that these frauds now go by the terminology, '419 scam', the name being derived from the fact that the section in the Nigerian penal code that deals with cheating is 419, says Thachankary. Police have arrested money mules in Mumbai, Delhi and Hyderabad, though none yet in Kerala, where more people have apparently sent money to mule accounts. In the biggest reported loss yet in the state, a Kannur man lost Rs 40 lakh, trusting e-mail promises. When caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.

Money mules play a prominent role in successful phishing attacks. The need for money mules arises because while a criminal in a developing country can obtain the credit card numbers, bank account numbers, passwords and other financial details of a victim living in the first world via the internet through techniques such as malware and phishing, turning those details into money usable in the criminal's own country can be difficult. With more and more business and monetary deals taking place over the Internet, instances of fraudulent transaction and identity thefts are bound to increase. It depends on the users to stay alert and avoid falling prey to this menace. These money mules are recruited in a very interesting fashion- the ads appear innocently on all major employment listing sites, offering stay-at-home positions titled; 'shipping manager', 'private financial receiver' or 'sales representative'. This is the other side of phishing that most people never see or hear about. But, it's probably the most important part of the attack. Without the money mule, phishers really can't do anything with stolen credit card credentials.

Effects for Financial Institutions

The following are several potential negative effects that money mule schemes have on financial institutions (FIs) related to financial losses, regulatory fines and reputational harm:

- **Fraud:** Money mules are just one part of a wider cybercrime scheme to defraud FIs and their customers. Because many banks have

zero-liability policies related to customer online banking, the FIs typically absorb the losses.

- **Money Laundering:** The specific actions taken by money mules to transfer or transport money to fraudsters is a money-laundering transaction. FIs in the United States, United Kingdom and other countries have faced increased regulatory scrutiny related to money laundering activity over the past decade. Recently in India HDFC bank has complained a case against money mule scam. A couple of other private sector banks have also come across the use of some of their account-holders as money mules for inward and outward transfer of fraudulently obtained money, but the names could not be confirmed. FIs are expected to have a robust money-laundering program and know-your-customer policies and procedures in place. Anti-money-laundering noncompliance regulatory fines can be substantial.
- **Reputation Risk:** FIs face damage to their reputations if they are caught up in a widespread money mule syndicate or are frequent targets of money mules due to weak account-opening controls. FIs may suffer a lack of confidence on the part of consumers from activity publicized in the popular press. Conversely, FIs with strong fraud and money-laundering-monitoring systems and advanced analytical tools may be able to enhance their reputation by identifying money mule rings and fraud activity and assisting law enforcement and prosecutors with investigations and successful convictions.

SUGGESTIONS TO PROTECT FROM E-FRAUD

1. Do not respond to emails asking for your bank account details.
2. For any overseas job offer, first confirm the identity and contact details of the employing company.
3. Do not get carried away by attractive offers/commissions or consent to receive unauthorized money.
4. The operations of such mule accounts can be minimized if RRBs follow the guidelines contained in various RBI circulars on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002. RRBs are, therefore, advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.
5. Indian banking industry will have to fight jointly and develop methods against this mess. Also need to pay more attention to educate its customers that can aid in smooth and secure means of net banking.

The consequences of being a money mule are:

- The bank will spot this unusual activity on your account. Mules typically have a lifespan of only one or two transfers before being detected.
- You will be liable to repay all the monies paid through your account.
- Your bank accounts will be frozen and you will be severely limited in your ability to open a bank account or access financial products in the future.
- You will damage your credit rating and potentially be black listed by the banks.

- You may be subject to criminal investigation and if found guilty, given a criminal record.

It's important to note that even if you have nothing to do with the actual theft of funds from another person's account, by enabling your bank account to be used in receiving and transferring such funds whether knowingly or unknowingly, you are acting illegally. By providing your personal and account information to criminals you may also be putting yourself at risk from identity fraud.

CONCLUSION

The concept of the money mule is not new. They have played an important role in fraud and money laundering for decades. Individuals who receive and transfer money or merchandise to third parties are mules that are needed to help clean or launder stolen money or goods. Some mules know, some don't, some suspect they are part of an illicit scheme and some are professional mules who offer their services for hire. Money mule scams are common in countries like the US and the UK. India is now on the fraudsters' radar possibly more because of liberalization of outward capital flows.

The output of this study can give people, authorities and organizations a better understanding of money mule scams happening in India. The study gives answers to some research questions that can help authorities and organizations to understand, prevent and stop phishing and the consequences of being a money mule. The recommendations and concerns may help future policy.

REFERENCES:

i. *www.hdfcbank.com*
ii. *https://www.rbi.org.in/*
iii. *World Bank. (5 1995). Money Laundering and International Efforts to Fight It. Accessed 12. 9. 2013 http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/ 282884-1303327122200/048scott.pdf.*
iv. *https://www.safeinternetbanking.be/en/fraud-techniques/money-mules*
v. *"The Most Common Schemes for Targeting the Unknowing Money Mule" by Brooke Satti in security intelligence .com*