A Preliminary Profiling of Internet Money Mules: An Australian Perspective

Manny Aston, Stephen McCombie, Ben Reardon, Paul Watters

Cybercrime Research Lab, Macquarie University

*m.aston@uws.edu.au, mccombie@comp.mq.edu.au, ben@cybercrime.com.au,
p.watters@ballarat.edu.au*

Abstract

Along with the massive growth in Internet commerce over the last ten years there has been a corresponding boom in Internet related crime, or cybercrime. According to research recently released by the Australian Bureau of Statistics in 2006 57,000 Australians aged 15 years and over fell victim to phishing and related Internet scams. Of all the victims of cybercrime, only one group is potentially subject to criminal prosecution: 'Internet money mules' – those who, either knowingly or unknowingly, launder money. This paper examines the demographic profile – specifically age, gender and postcode – related to 660 confirmed money mule incidents recorded during the calendar year 2007, for a major Australian financial institution. This data is compared to ABS statistics of Internet usage in 2006. There is clear evidence of a strong gender bias towards males, particularly in the older age group. This is directly relevant when considering education and training programs for both corporations and the community on the issues surrounding Internet money mule scams and in ultimately understanding the problem of Internet banking fraud.

1. Introduction

With the massive growth in Internet commerce in the last ten years there has been a corresponding boom in Internet crime. Criminals are using the borderless Internet to reach far from their home countries. Since 2003 a large portion of this crime has been fraud against Internet banks and their customers. Criminals compromise users credentials for various Internet Banks capturing their credentials by either getting the user to visit a fake banking site called a Phishing site or by using some malicious computer code (called a Trojan or crimeware) placed on the victim's machine to capture those details when victims go the real

banking website [8]. The criminals then use these credentials to log onto the victims accounts and illegally withdraw funds.

While the criminals can easily access Internet Banks and perform transactions from the other side of the world they cannot necessarily get the money into their own hands so easily. Some early Internet fraud used the Overseas Telegraphic Transfer (OTT) functionality of some Internet Banks to repatriate the fraudulently obtained funds directly to other countries. However the Internet Banks with this facility quickly began to limit this functionality or tightly scrutinize any transactions that did occur looking for suspicious recipients and the countries being used by criminals to receive funds. This created a problem for the criminals - how to get the money out of the victims' country. Out of this problem the "Internet money mule" was born. One of earliest known cases was in Australia. On Monday 17 March 2003 an email was sent out purporting to be from "admins at Commonwealth Bank" directing customers to a Florida hosted copy of the Commonwealth Bank Of Australia website, which is now known as a phishing site. A number of customers gave up their credentials to the website. Shortly after the credentials were used to transfer money to the account of a Tasmanian man who had been recruited on a Croatian Community website to receive the money and then transfer it to Eastern Europe. The Australian Federal Police subsequently arrested this man when he tried to draw some of the fraudulently obtained funds out of his own account. The man escaped prosecution at the time as he claimed he was unaware that the moneys were illegally obtained [7].

When the Internet fraud is investigated the Internet money mules are generally easily identified and any fraudulently obtained funds that may have been kept as the "commission" fee are recovered. It does not matter whether the Internet money mule is fully aware of the crime being committed or ultimately is just an innocent

agent as they rarely benefit from the crime. The criminals that recruit them do not care as the mules have served their purpose and pose no threat to the criminal enterprise. Thus in most cases the Internet money mules are expendable dupes for overseas criminals.

There is little meaningful data to show the extent of the problem of Internet money mules in Australia. A recent data source in regard to fraud more generally in Australia is the Australian Bureau of Statistics (ABS) Personal Fraud Survey [2], conducted throughout Australia during July to December 2007. According to the survey a total of 806,000 Australians aged 15 years and over were victims of at least one incident of personal fraud in the 12 months prior to interview. This equated to a victimisation rate for personal fraud of 5% of the population aged 15 years and over. There were 453,100 victims who lost money in the 12 months prior to interview, incurring a combined financial loss of almost one billion dollars (\$977 million). Of the victims who lost money to personal frauds, the median financial loss was \$450 per person, while the mean loss was \$2,156 per person.

While no other demographic research is available for incidences of Internet money mules there is data relating to fraud offenders more generally. In 2007 international tax and audit consultancy, KPMG, selected 360 cases of white collar fraud against the company identified by its own forensic division for analysis. Their findings were published in the "Profile of a Fraudster Survey 2007." [6] The survey concluded that in the corporate world, 70 per cent of white collar crimes are committed by people between 36 and 55 years; over 80 per cent of fraudsters are male; and members of senior management, including board members represent 60 per cent of all fraudsters. While Internet money mules are not necessarily fraudsters per se they may share some of the characteristics of them.

This paper examines the demographic profile – specifically age, gender and postcode residence – of 660 cases of confirmed money mule incidents during the calendar year 2007, for one major Australian financial institution. We compare them against 2006 ABS statistics of Internet usage [1] using as a null hypothesis the assumption that the age, gender and state of residence of money mules will mirror that of general Internet usage.

2. A Background to Internet Money Mule Scams

Online criminals who conduct phishing and Trojan attacks need Internet money mules to receive the fraudulently obtained funds into their bank accounts

for onward forwarding to the overseas based criminals [9]. These criminals advertise for Internet money mules through spam email, Internet messaging and both fraudulent and legitimate employment web sites. They claim to be legitimate employment opportunities with mules receiving between 7% to 10% of funds transferred via their accounts as a commission.

In Western Australia, the Department of Consumer and Employment Protection's 'WAScamNet' database recorded 1,709 employment and money mule email offers reported by consumers in October 2006 alone. This was 59 percent of all scam emails reported. This category represented the largest category of scam emails reported to the Department each month [3].

3. Anatomy of an Internet Banking Fraud

Figure 1 shows the relationship of the money mule to Internet banking fraud, and is an example of a typical Internet banking fraud. The first Phase in the Internet banking fraud involves the criminal sending a phishing email or Trojan infected or lure email to thousands of potential victims. A small percentage of those receiving a phishing email actually respond, usually by confirming their account details or in the other case are infected with a Trojan and have these details compromised when they conduct a real session with their Internet bank (Phase 2). Our victim in this example has 'clean money' (c\$) in their bank account. According to the ABS [2] in 12 months over 5.8 million Australians were exposed to phishing emails (this involved people receiving and viewing or reading an unsolicited invitation, request, notification or offer, designed to obtain their personal information or money or otherwise obtain a financial benefit by deceptive means), and of those 5.7% (or 329,000 people) became victims by responding to the scam by supplying personal information, money or both, or seeking more information.

In Phase 3, the potential mule is approached with a job offer, which is usually advertised by unsolicited spam email, Internet messaging and both fraudulent and legitimate employment web sites. Mules are recruited using job titles such as "Financial Managers", "Representatives", "Agents" or the like, and are typically promised a 7-10% fee for transferring funds. In order for the transfer to take place mules need to supply their current bank account details or if they choose set up a new account for this purpose supply those details (Phase 4). In Phase 5 the criminal transfers money from a compromised bank account into the mules account. The mule, simply doing what their 'job' requires, transfers this 'dirty' money (d\$) – minus their fee – via financial transfer services such as

Western Union to an overseas address (Phase 6). The Internet banking fraud now complete typically the Internet bank involved identifies the Internet money mule and recovers the fee from the mule. The mule may then be subject to prosecution if it can be proven that they laundered the proceeds of crime however this generally requires them to have the requisite guilty knowledge or at least be reckless to the fact.

Figure 1. Anatomy of an Internet fraud

4. Methodology

The data used in this paper has been obtained from de-identified database material gathered by the Internet fraud investigation team of a major Australian financial institution. As a basis of comparison, the ABS Patterns of Internet Access in Australia Survey 2006 [1] was used.

The data supplied by the financial institution is particularly relevant as it represents actual cases of Internet money mule activity – where the mules had willingly given their account details for the receipt of illegally obtained funds. Unlike survey data it is not subject to possible bias that is often evident in self-report statistics. It also represents a complete set of data, as it includes every case investigated by that financial institution for a calendar year (2007). While no doubt the financial institution's investigation database on money mules is extensive, the fields supplied to the authors were less detailed to maintain confidentiality: gender (male, female or joint account holder), age in years (whole numbers), and postcode. According to fraud investigators at the financial institution, each case was entered in the investigation database chronologically as each incident of fraud was discovered or reported to bank staff. [5]

The ABS Patterns of Internet Access in Australia Survey 2006 data represents numbers of people who have access to the Internet, based on the 2006 Census [1].

As the Internet money mule activity referred to in this paper involves those who have access to the Internet it is assumed that the demographic profile of money mules would mirror that of the general Internet user. Another hypothesis that they may otherwise mirror other Internet banking customers was discounted as investigators advised many of the Internet money mules were in fact new customers. [5]

The age categories selected were based on those used in the ABS survey. In the data set obtained by the financial institution there was a total of 130 people where the age was unknown. There ages were distributed in the sample population in the same ratio as the distribution for those with known age as 79 male and 51 female.

5. Results

A total of 660 accounts received illegally obtained funds. Of these 26 were in the name of joint account holders. For the purpose of this paper it was assumed that both account holders were money mules making the total number of money mules, 686. Table 1 represents the 686 money mules identified by the financial institution. In 71 cases there were multiple deposits made on different days.

Table 1. Internet money mules by age and gender by number

Age	Male	Female	Total
Under 15	6	6	12
15 - 24	88	45	133
25 - 34	142	84	226
35 - 44	85	69	154
45 - 54	60	44	104
55 - 64	29	10	39
65 - 74	13	0	13
75 +	5	0	5
TOTAL	428	258	686

Of the 686 money mules, 429 were male and 257 were female (Table 1). This meant in percentage terms males comprised 62.39% and females 37.61% (Figure 2). Of the 71 multiple instance of money mule activity, 53 were male and 21 were female.

Figure 2. Percentage break down of males and females from ABS statistics on Internet users compared to Internet Money Mules

5.1. Categorical Analysis of Mule Data

5.1.1. Sex Differences. The expected occurrence of male and female mules (all other things being equal) would be 343 each. Using a Pearson chi-square analysis, $\chi^2=21.91$, $df=1$, $p = <.0001$, so there are significantly more male mules than female mules overall.

5.1.2. Age x Sex Differences. A Pearson chi-square analysis was performed within the different age bands shown in Table 1. The results are summarized below:

- < 15 : $\chi^2=0.00$, $df=1$, $p = 1.00$, so there are no differences between males and females in this age range.
- $15-24$: $\chi^2=7.11$, $df=1$, $p = 0.0077$, so there are significantly more male mules than female mules in this age range.
- $25-34$: $\chi^2=5.48$, $df=1$, $p = 0.0192$, so there are significantly more male mules than female mules in this age range.
- $35-44$: $\chi^2=0.83$, $df=1$, $p = 0.3623$, so there are no differences between males and females in this age range.
- $45-54$: $\chi^2=1.24$, $df=1$, $p = 0.2655$, so there are no differences between males and females in this age range.
- $55-64$: $\chi^2=4.86$, $df=1$, $p = 0.0275$, so there are significantly more male mules than female mules in this age range.
- $65-74$: $\chi^2=6.03$, $df=1$, $p = 0.0141$, so there are significantly more male mules than female mules in this age range.
- $75+$: $\chi^2=3.61$, $df=1$, $p = 0.05$, so there are significantly more male mules than female mules in this age range.

5.1.1. Multiple Instances Sex Differences. The expected occurrence of repeat offender male and

female mules (all other things being equal) would be 35 each. Using a Pearson chi-square analysis, $\chi^2=7.08$, $df=1$, $p=0.0078$, so there are significantly more multiple instances male mules than female mules.

6. Discussion

Naturally there are statistical limitations to this work however the significance of the raw data cannot be underestimated. It is rare to obtain archival data sets such as this, and with this in mind, we seek to find any preliminary statistical trends and patterns, which emerge, many which warrant further investigation.

There is a strong gender bias towards Internet money mules being males. This is even greater when the element of potential criminal intent is introduced with multiple instances (In multiple instances the mules have usually been advised the nature of the fraud already). The bias progressively increases as the age of the money mule increases. The proposition that males are more prone to this type of risky endeavour is partly supported by the KPMG Survey [6], which indicated that in 85 percent of profiles fraudsters were male. However this survey was heavily influenced by frauds against the company often by insiders who were senior management or executives (roles where men often predominate).

Figure 3. Percentage break by age group from ABS statistics on Internet users compared to Internet Money Mules

Figure 3 shows a comparison of the financial institutions mule data against the ABS statistics for Internet usage across the various age categories. Of the money mules, people between 25 and 34 represented 32.94 percent of the total, while those aged between 35 and 44 a represented 22.45 percent. Over 55 percent of all money mules were aged between 25 and 44. The

low representation (1.75 percent) of young people aged between 5 and 14 (even though they are a significant percentage of the total internet users – 17.22 percent) is expected as it would be more difficult for minors to open bank accounts without parental or guardian consent.

In the 45 – 54 year old category the total number of mules are roughly consistent with the number of Internet users (16.65 percent versus 15.16 percent respectively). In the over 55, 65, and 75 categories mules are proportionally less than Internet users for the same categories.

Figure 4. Percentage breaks down of males and females by age groups from ABS statistics on Internet users compared to Internet Money Mules

Figure 4 shows the ABS and mule data age categories with gender highlighted. Apart from the equal distribution of mules in the Under 15 age group, there are significantly more males represented in every age category of the mule data. This difference is particularly evident in the 15 – 24 age range and in the 25 – 34 age groups. Of further interest is the complete absence of female mules in all age groups over 65.

6.1. Analysis of Mule Postcodes

In the data set supplied to researchers by the financial institution was the postcode of the Internet money mule accounts involved in 660 incidents in 2007. Using that data the percentage breakdown between States and Territories was calculated. Researchers then compared these percentages to the 2006 ABS figures for Internet users by State and Territory.

Figure 5. Postcodes of Internet money mules accounts mapped on Australia

Figure 6. Postcodes of Internet money mules accounts mapped on Sydney

Figure 7 shows the results of that comparison. While Queensland has a very similar percentage of mules to Internet users 20.09% to 20.69% the two most populous and with the largest urban centres NSW and Victoria account for a larger portion of the mules than Internet users. With NSW being 34.76% of the mules compared to 32.59% of the ABS Internet users and more significantly Victoria being 33.19% of the mules to 24.73% of the ABS Internet users. All the remaining states and territories representing fewer Mules than the ABS Internet users. Western Australia

being 6.42% of the mules compared to 10.17% of the ABS Internet users. South Australia being 3.29% of the mules compared to 7.49% of the ABS Internet users. Tasmania being 0.94% of the mules compared to 2.20% of the ABS Internet users and finally Northern Territory being 0.16% of the mules compared to 0.75% of the ABS Internet users.

Figure 7. Percentage break down by state and territory from ABS statistics on Internet users compared to Internet Money Mules

While one needs to exercise caution with drawing broad conclusions from this it does raise the possibility that those in populous states with large urban centres like Sydney and Melbourne are more prone to becoming mules. This will however require further research to establish. Further work is currently underway to create a heat map of these postcodes and to examine trends between urban and rural areas of each state and territory and of Australia as a whole. To illustrate the potential of this future work Figure 5 maps the mule postcodes on a map of Australia and Figure 6 on a map of the Sydney metropolitan area.

7. Conclusion

While this analysis is really preliminary and there is more work to be done to fully exploit the data it already does present a number of areas for future research. A clear trend is the over representation of males particularly in the 25-34 age group and in older age ranges where males predominate. The Internet money mule data needs to be further investigated in

conjunction with similar profiling such as the work by KPMG [6].

While the size of the sample is small (some 660) it is the first look at Internet money mules as a group and is actual incident data rather than based on surveys. When compared to other human factors research in the cybercrime area such as Dhamija's "Why Phishing Works" [4] where the sample size was a paltry 22, the sample is actually quite large.

The geographical data itself needs further analysis and this will also form the basis of future research. Whether the differences in locality between the ABS Internet users and Internet money mule data are significant still needs to be shown. Of particular interest would be looking at whether there are any differences between urban and rural communities.

The key lessons from this research and subsequent work is to better understand Internet money mule profiles so education can be targeted to those individuals and to better educate bank staff to identify those setting up accounts to be Internet Money Mules.

While this demographic data does clearly help in this regard other profile elements need to be looked at in future research. These could include such things as profiling how Internet money mule accounts are established and operated in contrast to other account establishments.

8. References

- [1] Australian Bureau of Statistics, "Patterns of internet access in Australia, 2006", ABS, Canberra, 2007.
- [2] Australian Bureau of Statistics, "Personal Fraud, 2007", ABS, Canberra, 2008.
- [3] Australian Institute of Criminology, "Money Mules", High Tech Crime Brief 16, 2007, Retrieved 23 March, 2008.
- [4] Dhamija, R., Tygar, J.D., and Hearst, M. "Why Phishing Works." In Proceedings of the CHI 2006. Montréal, Québec, Canada, 2006
- [5] Interview with subject Financial Institutions Internet Security Team (2008). Conference call phone interview.
- [6] KPMG, "Profile of a Fraudster Survey 2007", KPMG International, Location, 2007. Retrieved 20 January, 2009.
- [7] S. McCombie, "Trouble in Florida: The Genesis of Phishing attacks on Australian Banks", 6th Australian Digital Forensics Conference Perth 2008.
- [8] S. McCombie, P. Watters, A. Ng, B. Watson, "Forensic Characteristics of Phishing - Petty Theft or Organized Crime?" Proceedings of WEBIST, 149-157
- [9] A. Stabek, S. Brown, & P. Watters, "The Case for a Consistent Cyberscam Classification Framework (CCCF)", Proceedings of the Cybercrime and Trustworthy Computing Workshop (CTC-2009).